Managing Skype for Business:
QoS with LiveNX

Product Disclaimer: LiveAction has renamed their software solution, formerly known as “LiveAction” to “LiveNX.” From 2016 and on, LiveNX will remain the official name for the software solution.

TABLE OF CONTENTS

MICROSOFT SKYPE FOR BUSINESS OVERVIEW

Microsoft© Skype© for Business (formally known as Lync©), part of Microsoft Office 365, is an enterprise-level collaboration solution for instant messaging, presence, conferencing, file sharing, and telephony. While Skype for Business is a simple application to use, protecting Skype voice and video call quality throughout the network can be difficult. Fortunately, a network administrator can effectively implement Quality of Service (QoS) protection for Skype using LiveAction's application-aware network performance management solution, LiveNX.

LiveNX utilizes Cisco's advanced features to simplify implementation of these management controls through a rich Graphical User Interface (GUI). LiveNX provides a comprehensive management solution for monitoring, troubleshooting and provisioning Skype QoS to ensure that bandwidth is properly allocated to support your enterprise's needs. Users can take advantage of LiveNX to virtually go back in time to perform analysis and troubleshooting for real-time or historic Skype calls utilizing the Medianet Performance Monitor Path Analysis feature.

This document describes how you can easily protect critical Skype audio and video traffic throughout the network with LiveNX. You'll learn how to:

- Configure Skype audio and media ports and markings at the Clients and Server
- Use LiveNX to verify Skype traffic through the network
- Use LiveNX to create Access Control Lists (ACLs) for Skype
- Use LiveNX to configure QoS Marking Policy
- Use LiveNX to configure QoS Queuing Policy
- Use LiveNX to monitor performance of Skype

By using NBAR2 (protocol pack 12 or higher), Cisco's application recognition technology built into IOS, Skype QoS management can be further simplified to uniquely identify Skype audio and video without having to configure Microsoft Skype Servers for QoS, Microsoft Group Policies for QoS, or build and manage complex ACLs in the network infrastructure.* This can translate to 50% faster (or higher) QoS deployments and reduces the chance of mistakes during the configuration. LiveAction highly recommends updating to this protocol pack to simplify a Skype QoS deployment (see Appendix D for further details).

MICROSOFT SKYPE AND THE ROLE OF QOS

Microsoft Skype is an application that allows enterprise users to communicate via instant messaging (IM), presence, audio/video conferencing, IP telephony, and collaboration tools. Communication occurs between Skype clients that have installed the Skype software on their PC, MAC or mobile devices (Windows, iPhone/iPad, Android). Other communication devices may also communicate via Skype (PSTN, IP phones, IP video conference unit). The enablement of these communication technologies is dependent on several Skype servers. Each server has a specific role in the Skype operation. The roles can be co-located on one server or installed on multiple servers to add high availability and scaling capabilities. These roles are:

- Front-End Servers
- Back-End Servers
- Mediation Servers
- Edge Servers

By default, Skype clients and servers do not set QoS markings on their data. Additionally, Skype client-to-client communication does not use a defined range of TCP/UDP ports. Since the network infrastructure cannot recognize Skype traffic by port or QoS marking in its default state, it cannot prioritize these flows as they traverse the network.* This can cause performance impact to both Skype voice and video traffic on highly utilized enterprise networks.

To ensure Skype always receives the QoS priority it needs, it must first be configured to set QoS markings on its traffic as it is sent onto the network. Microsoft has published white papers on their website for enabling QoS on Skype traffic. Visit here for more details.

These documents can be summarized into two primary steps:

1. Set uniform TCP/UDP port ranges that Skype applications will utilize
2. Set QoS markings on Skype clients and servers based on the port ranges above

This means that network administrators must configure the appropriate QoS markings by application (VOIP, VIDEO, etc.) for each client and server that participates in a Skype solution. There are three types of Skype communications: client-to-client, client-to-server, and server-to-server. Each application must be configured for these communications scenarios. Fortunately, centrally configured shell commands and Microsoft Group Policy can manage these configurations.

Once the Skype clients and servers have been configured to set the appropriate QoS markings for Skype data, the network infrastructure that these applications traverse must also be configured to support the level of call quality required to meet business objectives. This is done by the configuration of IP QoS to all applicable network devices (routers and switches) that transmit and receive Skype voice and video.

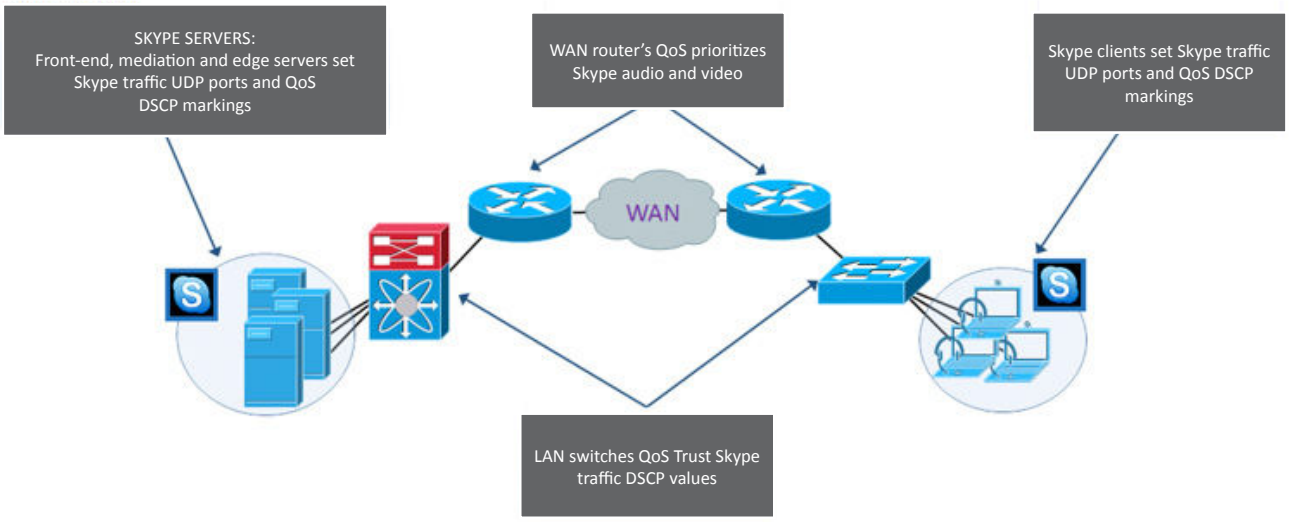
The management and configuration of QoS in networks can be very complex to operate, manage and validate. It can require reviewing hundreds of lines of Command Line Interface (CLI) commands to understand the configuration and performance of QoS polices on just one device alone. Therefore, understanding end-to-end QoS policies on an enterprise network can become extremely difficult at best. LiveNX has been designed to streamline the implementation and management of QoS in network environments and can be used to easily deploy this complex set of technologies to the network infrastructure.

*Cisco has updated its NBAR2 application recognition technology to granularity recognize Skype audio and video. By using NBAR2 protocol pack 15 (or higher) on the application Cisco routers and LiveNX, it is possible to easily protect Skype audio and video via just the network infrastructure. This means it is possible to eliminate the need for any changes on Microsoft servers or clients as outlined in this document (see Appendix D for further details).

This document will provide the configuration parameters required to configure Skype for Business 2016 clients and servers. It will also detail the required steps of implementing QoS in a network infrastructure. Finally, this document will highlight how a network infrastructure's QoS can be configured, monitored and validated using LiveAction software.

Microsoft Skype QoS Design

The following diagram shows a typical Skype enterprise deployment.



Define TCP/UDP Port Ranges

The first step in deploying QoS for Skype is to define the TCP and UDP port numbers that the Skype applications will use. These port numbers should be configured in a consistent way so all devices that participate in Skype will use the same ports for each application type–for example, VOIP could always use ports 20000-2099, video 21000-21099, etc.

Client-to-Client Settings

To configure client-to-client port use, you can use the following shell commands on the Skype Front-End Server. Once these parameters have been set, Skype clients should log off and back on to the Skype client to acquire these new settings. The following commands are a valid example of how to configure these settings:

```
Set-CsConferencingConfiguration -ClientMediaPortRangeEnabled $True
Set-CsConferencingConfiguration -ClientAudioPort 20000 -ClientAudioPortRange 100
Set-CsConferencingConfiguration -ClientVideoPort 20100 -ClientVideoPortRange 100
Set-CsConferencingConfiguration -ClientAppSharingPort 20200 -ClientAppSharingPortRange 100
Set-CsConferencingConfiguration -ClientFileTransferPort 20300 -ClientFileTransferPortRange 100
```

These can be entered via: Start > All Programs > Microsoft Skype Server 2016 > Skype Server Management Shell

Microsoft Skype Phone Edition Settings

The default QoS DSCP value of Skype Phone Edition is 40. In most environments the DSCP value for audio traffic is 46. To update this configuration, issue the following command:

```
Set-CsUCPhoneConfiguration -VoiceDiffServTag 46
```

This can be entered via: Start > All Programs > Microsoft Skype Server 2016 > Skype Server Management Shell

Microsoft Skype Server Settings

To configure client-to-server and server-to-server port use, you could use the following shell commands on the Skype Front-End Server. These settings update the Skype Conference, Application, and Mediation servers. Once these parameters have been set, the appropriate Skype services will need to be restarted to apply these new settings. The following commands are a valid example of how to configure these settings:

```
Set-CsConferenceServer -Identity <ConferenceServer:FQDN of Skype Pool> -AudioPortStart 21000
-AudioPortCount 1000
Set-CsConferenceServer -Identity <ConferenceServer:FQDN of Skype Pool> -VideoPortStart 22000
-VideoPortCount 1000
Set-CsConferenceServer -Identity <ConferenceServer:FQDN of Skype Pool> -AppSharingPortStart 23000
-AppSharingPortCount 1000
Set-CsApplicationServer -Identity <ApplicationServer:FQDN of Skype Application Srv. Pool>
-AudioPortStart 21000 -AudioPortCount 1000
Set-CsMediationServer -Identity <MediationServer:FQDN of Skype Mediation Srv. Pool> -AudioPortStart
21000 -AudioCount 1000
```

These can be entered via: Start > All Programs > Microsoft Skype Server 2016 > Skype Server Management Shell

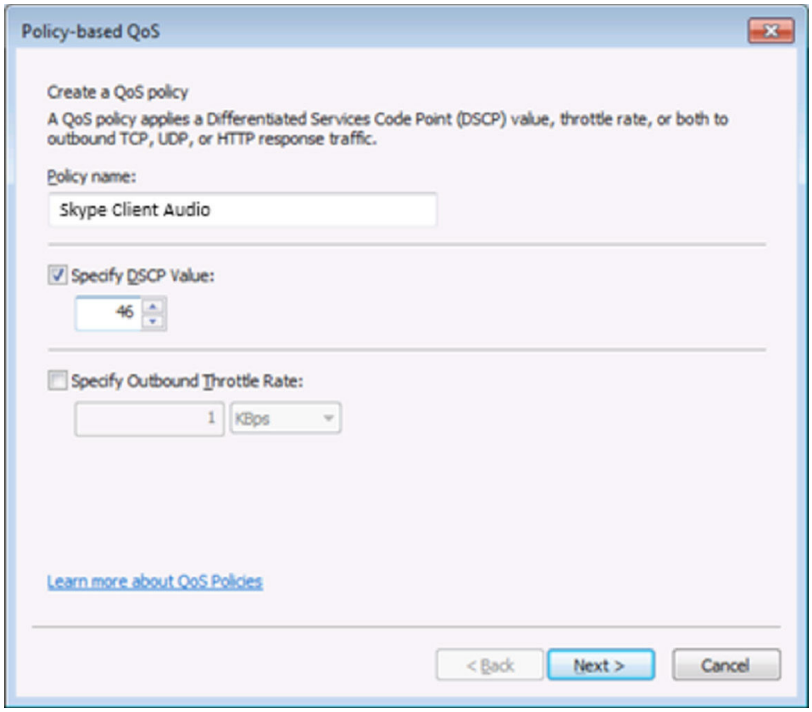
MICROSOFT SKYPE EDGE SERVER SETTINGS

The Skype Edge servers do not need to have any ports reconfigured, as they will rely on the other Skype devices inside the network for port selection. Note that DSCP markings only need to be set for private Skype traffic. Any DSCP values marked on Skype traffic that traverse the Internet will typically have these priority settings ignored by all service providers.

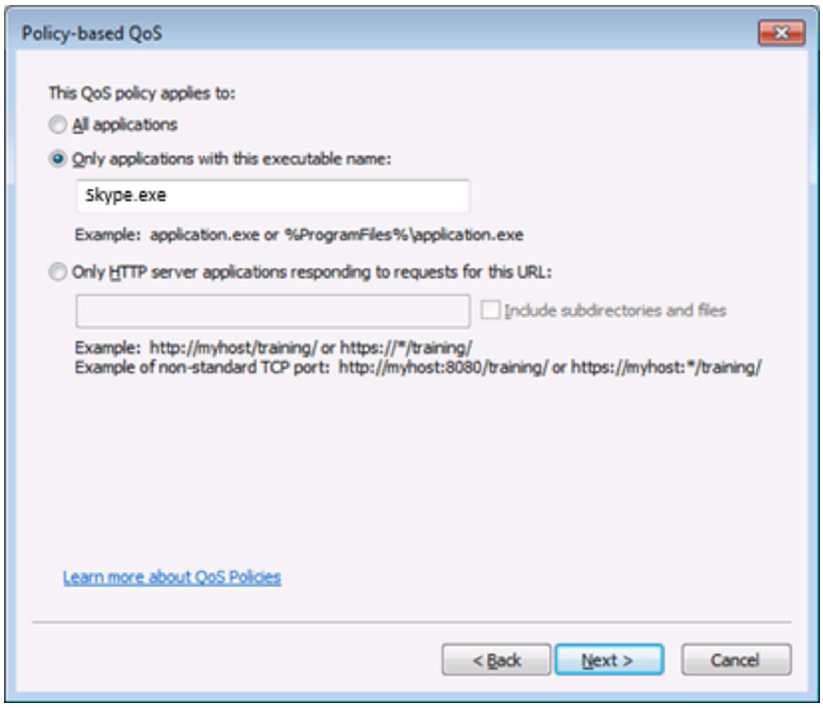
Define Group Polices

Once the Skype port settings have been assigned to all applicable device types via the Skype Server Management Shell, DSCP markings can be set by implementing Group Polices for these applications' port ranges. To implement a QoS Group Policy, navigate to a computer that has Group Policy Management installed, locate the container where the new policy should reside (e.g. client OU), right-click on the container and select "Create GPO in this domain, and link it here." The following screenshots will display how to configure the appropriate Group Policy for Skype Audio. This is applicable for Windows 7, 8, and Vista clients.

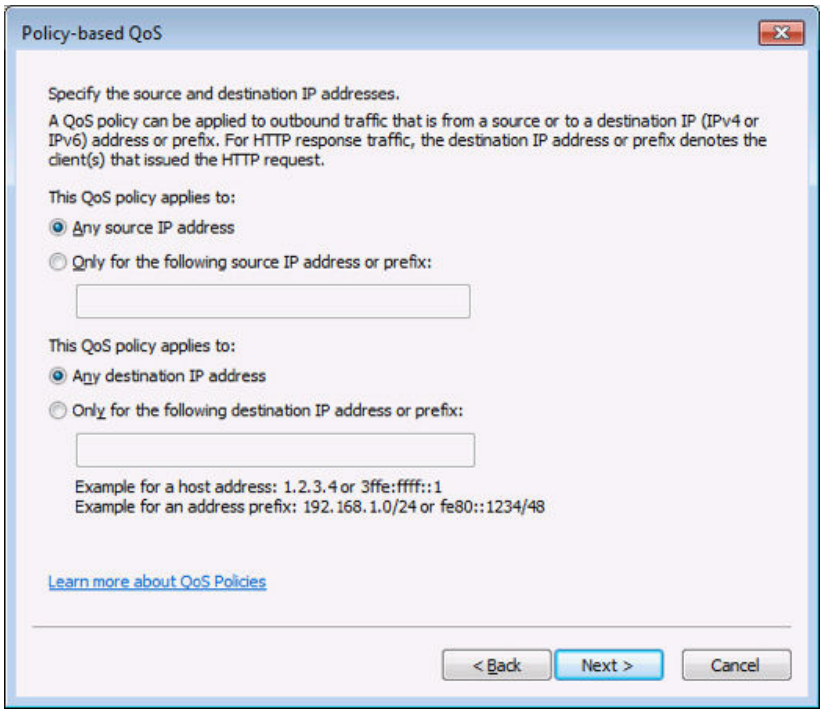
First, name the policy and specify the DSCP value.



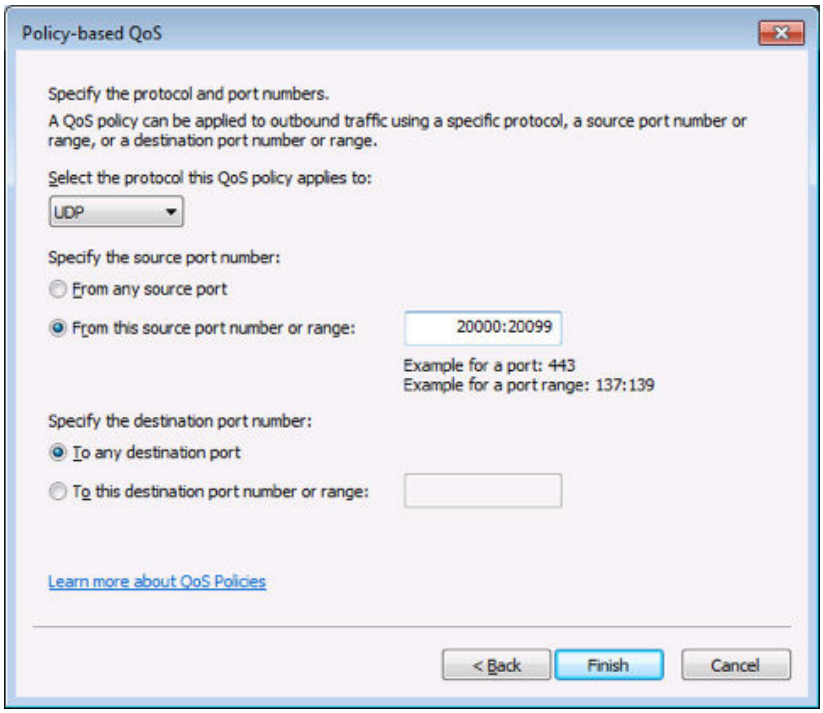
Define the application to which this policy applies.



Specify the source and destination address to which this policy applies.



Select the protocol and port ranges that this policy matches with and click “Finish.”



Microsoft Skype DSCP Marking Group Policies

The same process will need to be repeated for all other Skype clients and servers (Conferencing, Mediation, Application). Please use the table below as a sample reference for defining Skype TCP/UDP ports and Group Polices. The port numbers used in this example would be valid for an environment with up to 500 simultaneous conference users.

Group Policy Name	Application Executable	DSCP	TCP/UDP	Src IP	Dst IP	Src Ports	Dst Ports
Skype Conferencing Server Audio	AVMCUSvc.exe	46	Both	Any	Any	21000-21999	
Skype Conferencing Server Video	AVMCUSvc.exe	34	Both	Any	Any	22000-22999	
Skype Edge-Server Internal Audio–Clients	MediaRelaySvc.exe	46	Both	Edge Internal IP	Any		20000-20099
Skype Edge-Server Internal Audio–Servers	MediaRelaySvc.exe	46	Both	Edge Internal IP	Any		21000-21999
Skype Edge-Server Internal Video–Clients	MediaRelaySvc.exe	34	Both	Edge Internal IP	Any		20100-20199
Skype Edge-Server Internal Video–Servers	MediaRelaySvc.exe	34	Both	Edge Internal IP	Any		22000-22999
Skype Mediation Server Audio	MediationServerSvc.exe	46	Both	Any	Any	21000-21999	
Skype Application Server	OcsAppServerHost.exe	46	Both	Any	Any	21000-21999	
Skype Client Audio	Skype.exe	46	Both	Any	Any	20000-20099	
Skype Client Audio 2010	Communicator.exe	46	Both	Any	Any	20000-20099	
Skype Client Video	Skype.exe	34	Both	Any	Any	20100-20199	
Skype Client Video 2010	Communicator.exe	34	Both	Any	Any	20100-20199	

Note: These ranges may not be appropriate for all network designs.

NETWORK QOS CONFIGURATION

Microsoft Skype relies on the network infrastructure to honor and queue its traffic for call quality protection. The following pages will describe the steps required to implement and validate these QoS polices in a network infrastructure using LiveNX.

How Does QoS Work?

QoS is a suite of technologies used to manage bandwidth usage as data crosses computer networks. Its most common use is for the protection of real-time voice or video communications and high-priority data applications. QoS technologies, or tools, each have specific roles that are used in conjunction with one another to build end-to-end network QoS policies.

The two most common QoS tools used to handle traffic are classification and queuing. Classification identifies and marks traffic to ensure network devices know how to identify and prioritize data as it traverses a network. Queues are buffers in devices that hold data to be processed. Queues provide bandwidth reservation and prioritization of traffic as it enters or leaves a network device. If the queues are not emptied (due to higher priority traffic going first), they overflow and drop traffic.

Policing and shaping are also commonly used QoS technologies that limit the bandwidth utilized by administratively defined traffic types. Policing enforces bandwidth to a specified limit. If applications try to use more bandwidth than they are allocated, their traffic will be remarked or dropped. Shaping defines a software set limit on the transmission bandwidth rate of a data class. If more traffic needs to be sent than the shaped limit allows, the excess will be buffered. This buffer can then utilize queuing to prioritize data as it leaves the buffer.

The Weighted Random Early Discard (WRED) technology provides a congestion avoidance mechanism that will drop lower priority TCP data to attempt to protect higher priority data from the adverse effects of congestion.

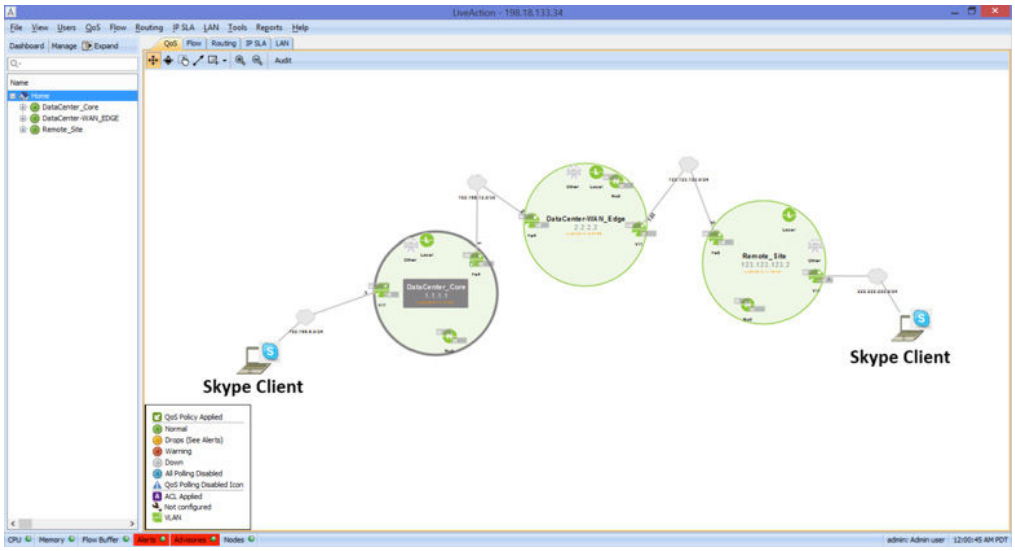
Finally, link-specific fragmentation and compression tools are used on lower bandwidth WANs to ensure real-time applications do not suffer from high jitter and delay.

Table 1: Packet flow through a typical QoS policy

WHAT IS LIVENX?

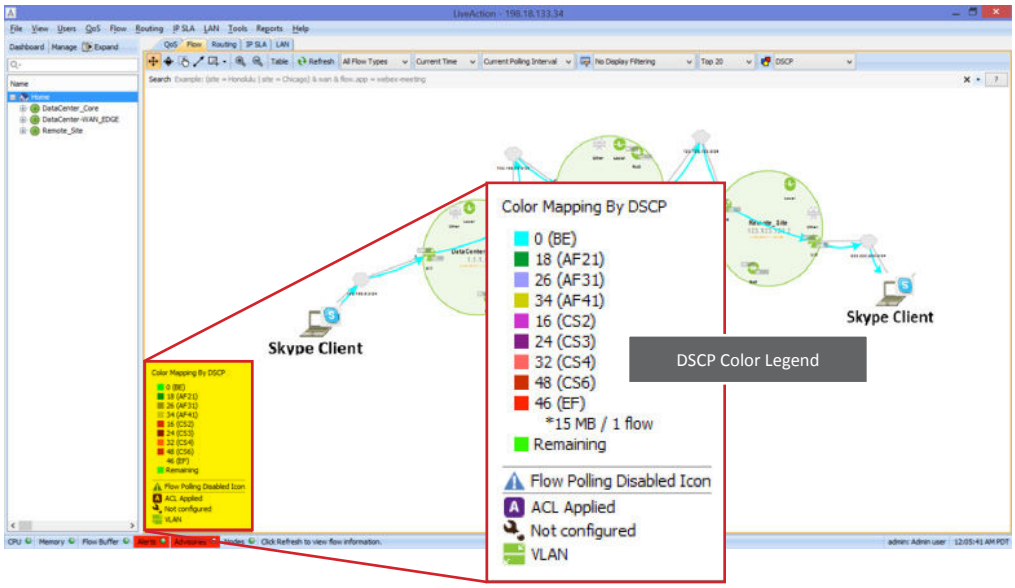
LiveNX is an application-aware network performance management tool that will graphically display how networks and applications are performing using SNMP and the latest advanced NetFlow capabilities now embedded in Cisco devices. In addition to showing application and network performance, LiveNX provides the ability to control application performance via its graphical QoS management capabilities. In the following, LiveNX will be used to highlight how easily QoS can be configured to manage and control Skype audio and video traffic. Moreover, this document will describe how LiveNX can be used to confirm the application performance of Skype using the latest Performance Monitoring technology now available in some Cisco devices.

The image below is a view of the LiveNX console. It shows a network diagram consisting of two Skype clients and three network devices. The three larger green circles represent routers and switches managed by LiveNX. The little green circles within the devices represent their interfaces.



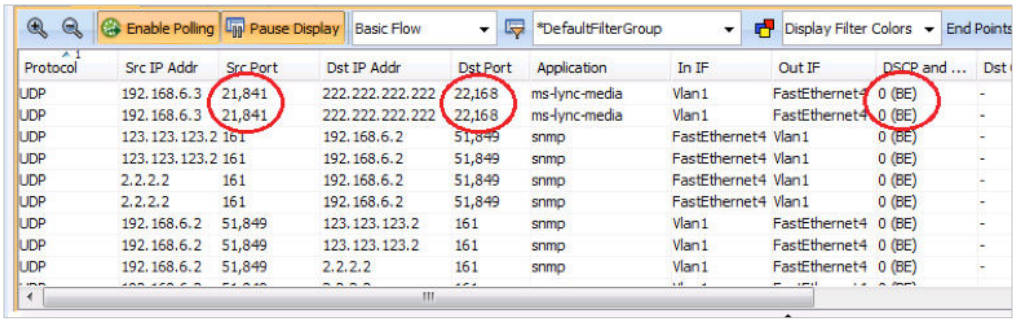
Microsoft Skype Audio QoS Classification with LiveNX

Since LiveNX is also a NetFlow collector, it has the ability to graphically visualize the traffic that is flowing over the network. In the diagram below, the light blue arrows represent Skype audio traffic traversing the network. In this example, the color legend below shows that the light blue arrows represent Best Effort traffic. This is what one would expect to see before any



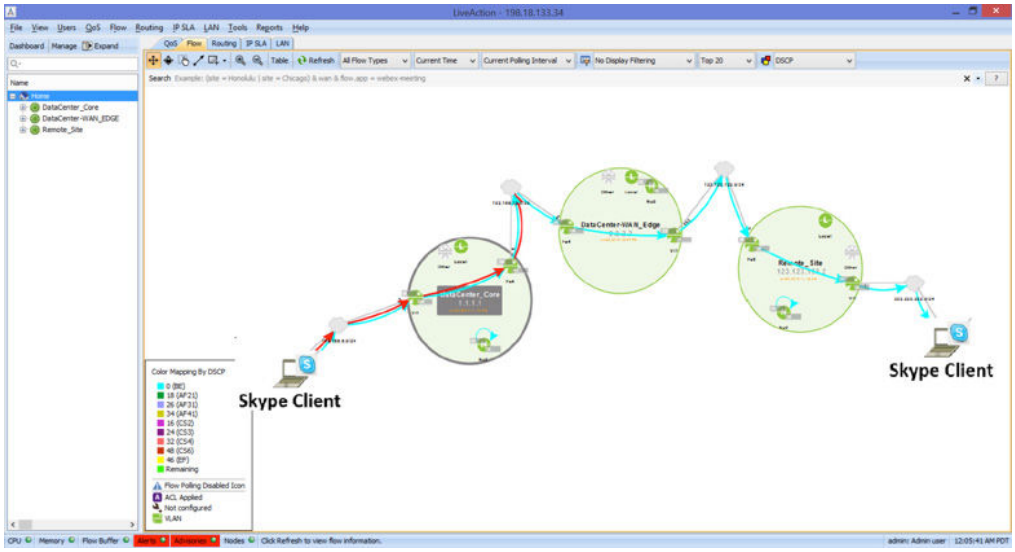
QoS configuration is implemented on the Skype servers and clients as described previously in this document.

Double-clicking on any of the larger circles (routers/switches) in the LiveNX network diagram will show the real-time NetFlow data of traffic that is flowing through the device. In the example below, the Skype traffic's UDP port numbers are not in the administrator's defined port ranges and the DSCP values are Best Effort. This confirms that the Skype servers and clients have not yet be been configured appropriately for QoS.

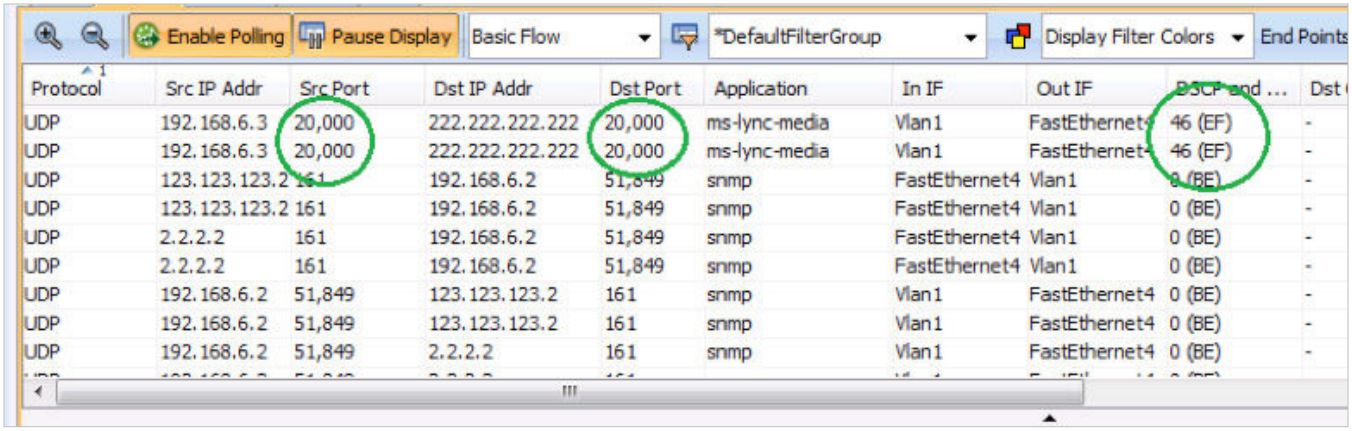


Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	In IF	Out IF	DSCP and ...	Dst
UDP	192.168.6.3	21,841	222.222.222.222	22,168	ms-lync-media	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.3	21,841	222.222.222.222	22,168	ms-lync-media	Vlan1	FastEthernet4	0 (BE)	-
UDP	123.123.123.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	123.123.123.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	2.2.2.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-

After the appropriate Skype QoS settings have been implemented on the Skype servers and clients, the network diagram will show red arrows, in addition to the light blue arrows. This indicates EF or high priority markings are now being set on Skype audio traffic. But notice in the example below, the red arrows are not being drawn through the whole Skype conversation path. This indicates that the network infrastructure's QoS trust policy is not configured correctly.

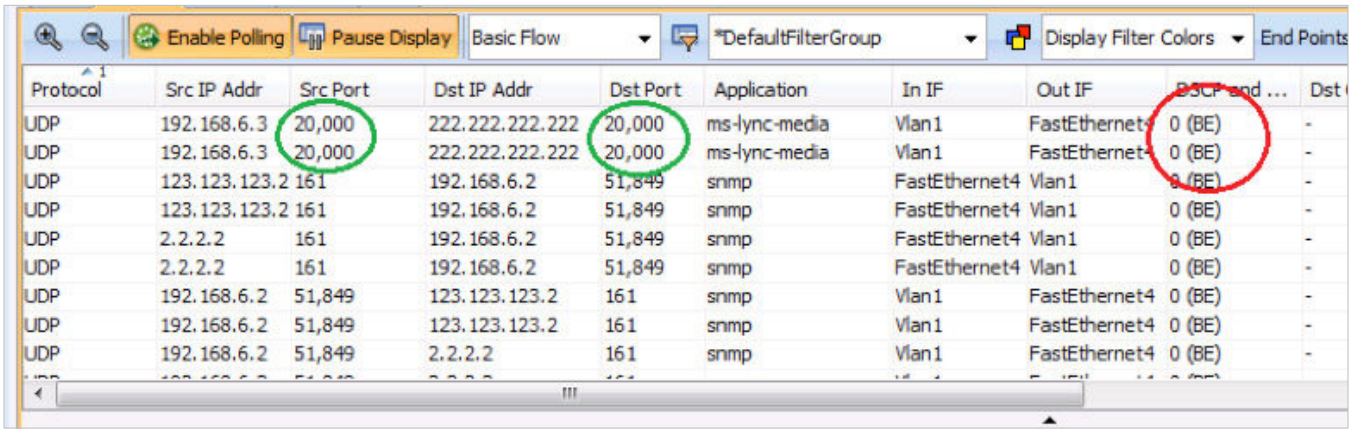


This can be confirmed if one was to double-click on the device that is showing the red arrows painted through it. In the LiveNX real-time NetFlow view below, the UDP ports are in the appropriate range and the DSCP value is EF.



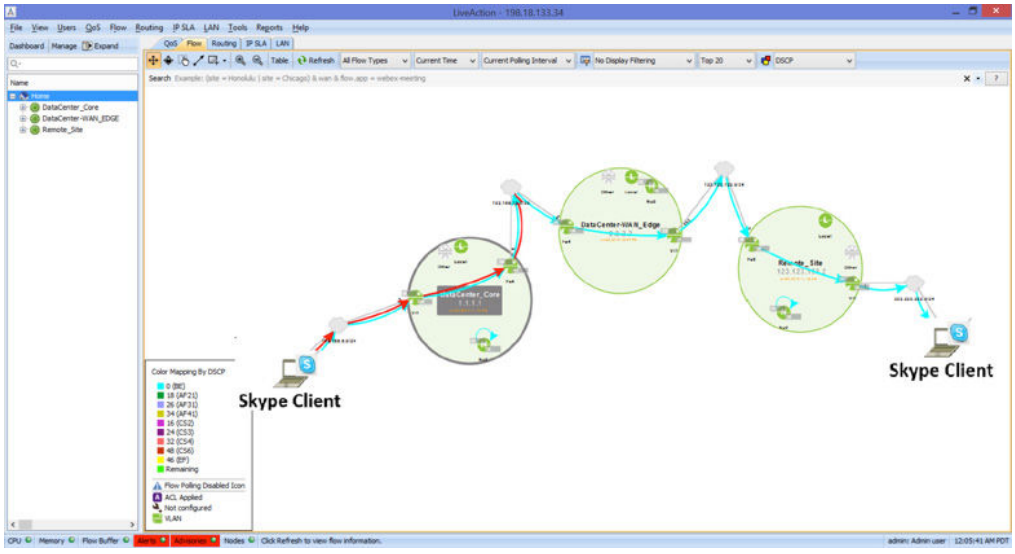
Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	In IF	Out IF	DSCP and ...	Dst
UDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan1	FastEthernet4	46 (EF)	-
UDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan1	FastEthernet4	46 (EF)	-
UDP	123.123.123.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	123.123.123.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	2.2.2.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-

If instead one double-clicked on one of the devices showing just blue arrows, the UDP ports would be in the appropriate ranges, but the DSCP value would still be 0.

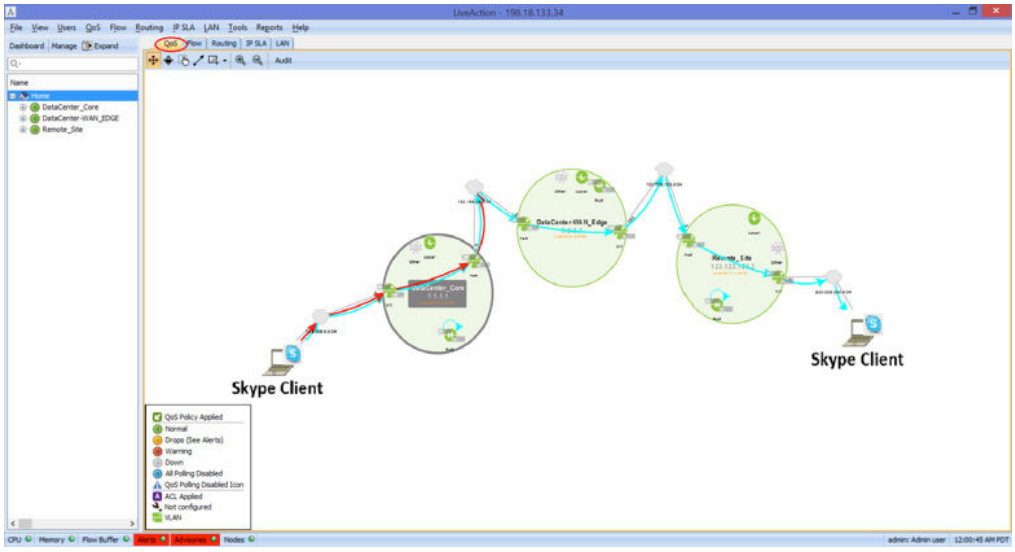


Protocol	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Application	In IF	Out IF	DSCP and ...	Dst
UDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.3	20,000	222.222.222.222	20,000	ms-lync-media	Vlan1	FastEthernet4	0 (BE)	-
UDP	123.123.123.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	123.123.123.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	2.2.2.2	161	192.168.6.2	51,849	snmp	FastEthernet4	Vlan1	0 (BE)	-
UDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	123.123.123.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-
UDP	192.168.6.2	51,849	2.2.2.2	161	snmp	Vlan1	FastEthernet4	0 (BE)	-

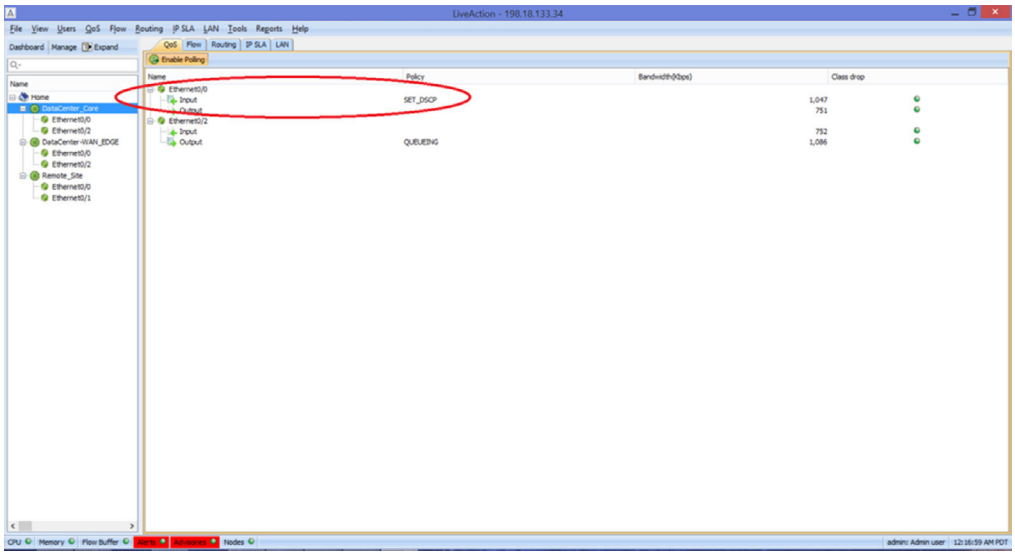
The previous screenshots validate what the LiveNX network diagram was indicating; the DSCP value of 46(EF) is being lost by some type of misconfigured QoS trust policy in the network. To investigate this network QoS issue further, the administrator should start the troubleshooting process on the last device that shows the intended QoS markings. In this example, this would be the first device on the left with the red arrows passing through it (shown below). Fortunately the LiveNX application doesn't stop at just showing the Skype QoS problems, but gives administrators the ability to fix the QoS issue with its graphical QoS management tools.



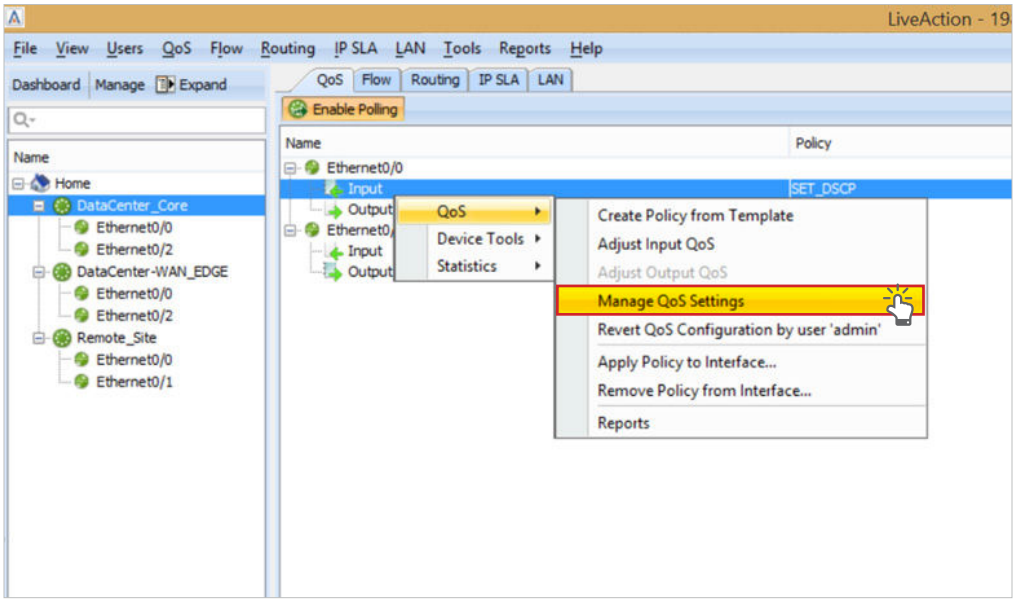
To access these tools, click the “QoS” tab at the top left of the LiveNX network diagram and then double-click on the device that needs QoS configuration investigation (the device to the left in this example).



This will show a list of interfaces managed on this device. Notice in the screenshot below that on the Ethernet 0/0 interface, there is a QoS policy named “SET_DSCP” configured in the input direction.

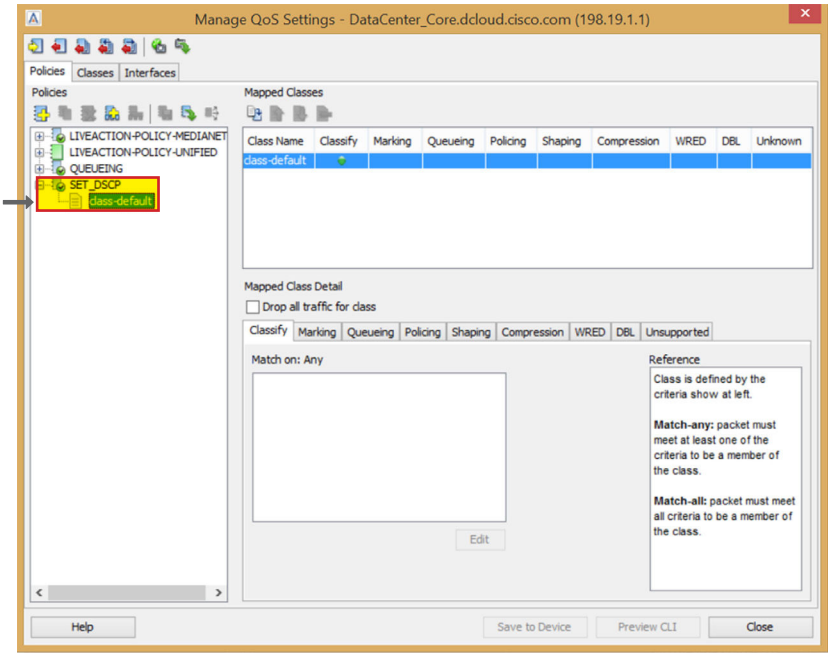


To further investigate this policy, right-click on the policy's name > select QoS > Manage QoS Settings.

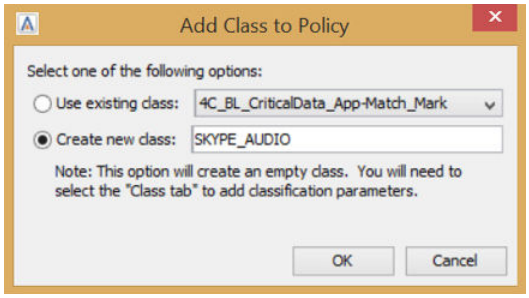


This will bring up a new window (shown below) that will allow the administrator to configure all required QoS policy settings via LiveNX's GUI.

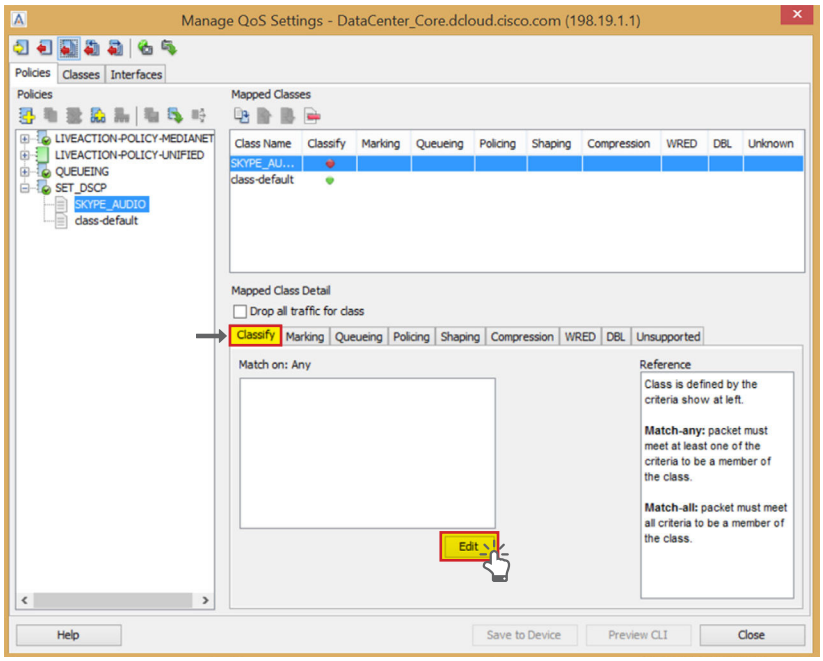
Select the policy named "SET_DSCP" in the list to the left. This will show a list of the classes applied to this policy. In this example, there is only one class named class-default. Click on "class-default" to highlight it. Notice how this policy is currently marking all traffic (via the class-default) with a DSCP value of 0, Best Effort.



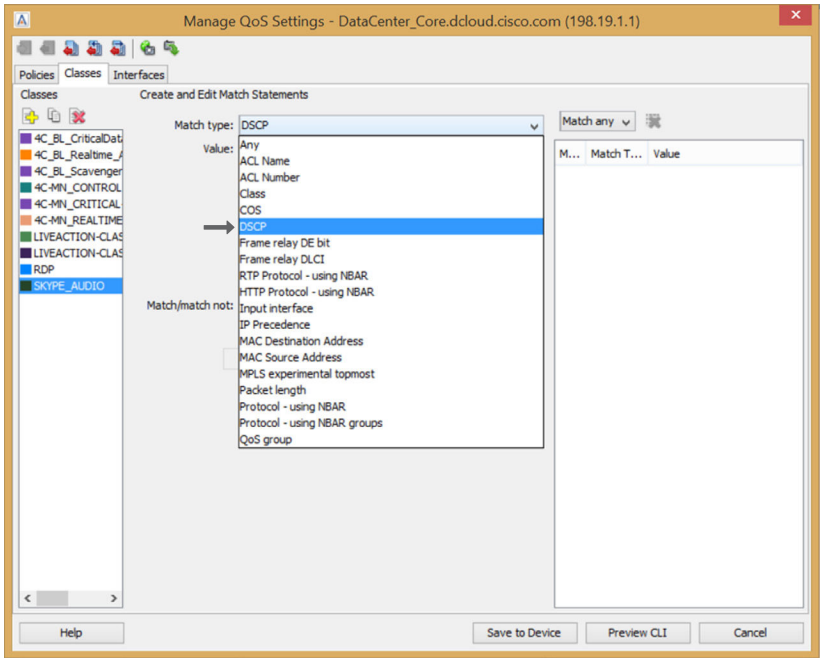
This policy needs to be fixed to allow Skype traffic's DSCP markings to pass through this device unchanged— that is, the DSCP value of 46 will be seen across all infrastructure devices to ensure consistent QoS handling of Skype traffic across the network. To do this, first right-click on the "SET_DSCP" policy and select "Add Class to Policy." This will bring up a new window, as shown below. Create a new class called "SKYPE_AUDIO."



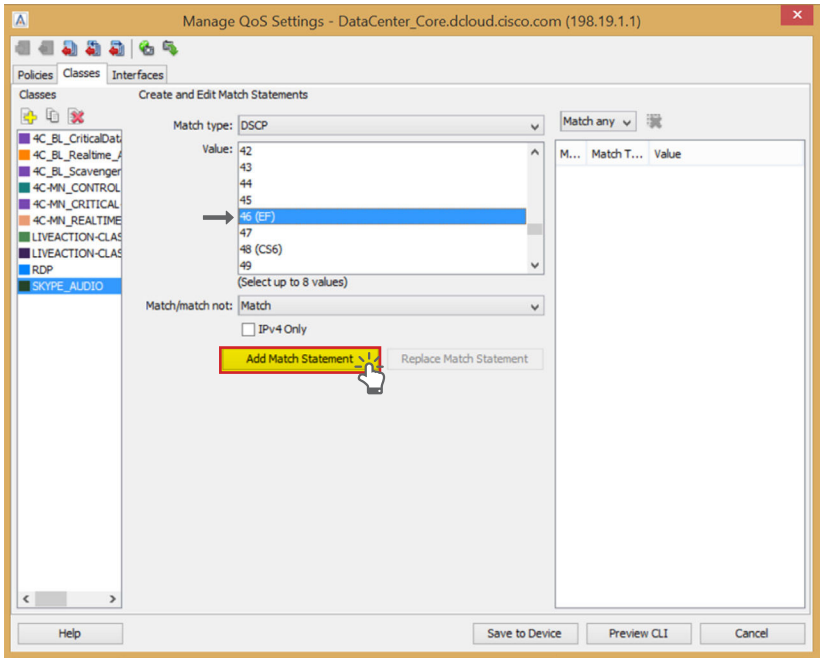
The new class will be added to the SET_DSCP policy. Match criteria needs to be defined to ensure the appropriate traffic uses this class. Click the "Edit" button on the "Classify Tab."



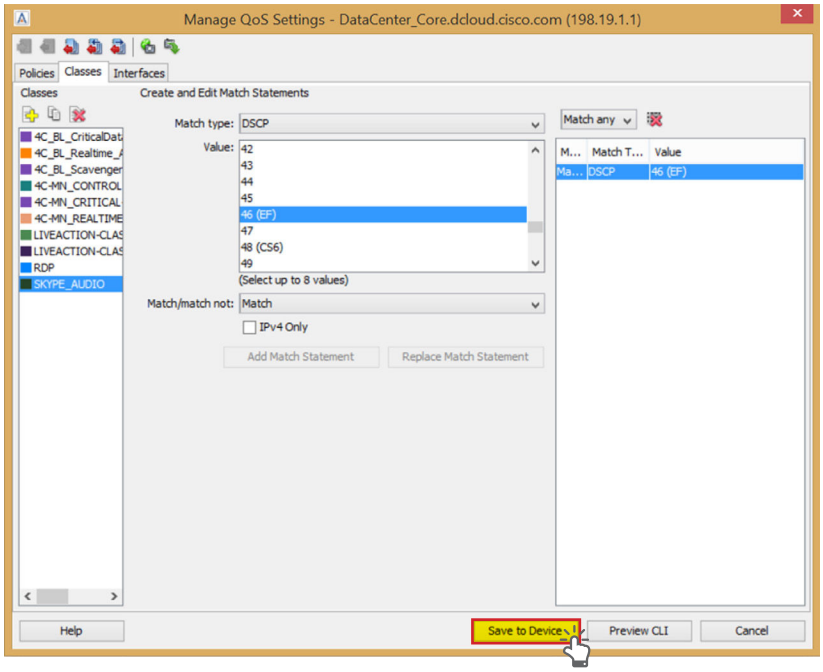
This will bring up the “Create and Edit Match Statements” configuration page. Select “DSCP” from the “Match Type” drop-down.



Select a “Value” of “46(EF)” and click “Add Match Statement.”

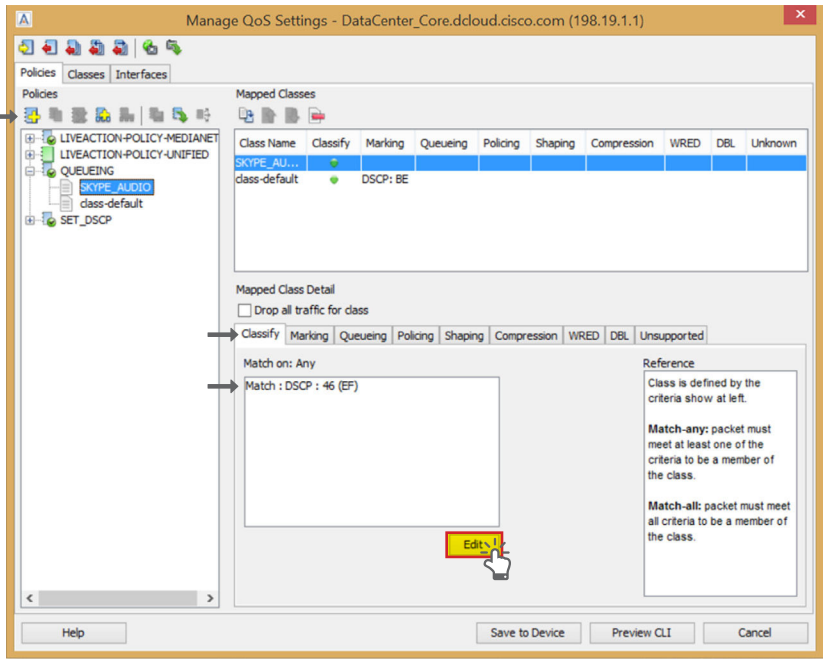


The DSCP value will now appear in the far right column, indicating it is a valid match type for this class. Click “Save to Device.”

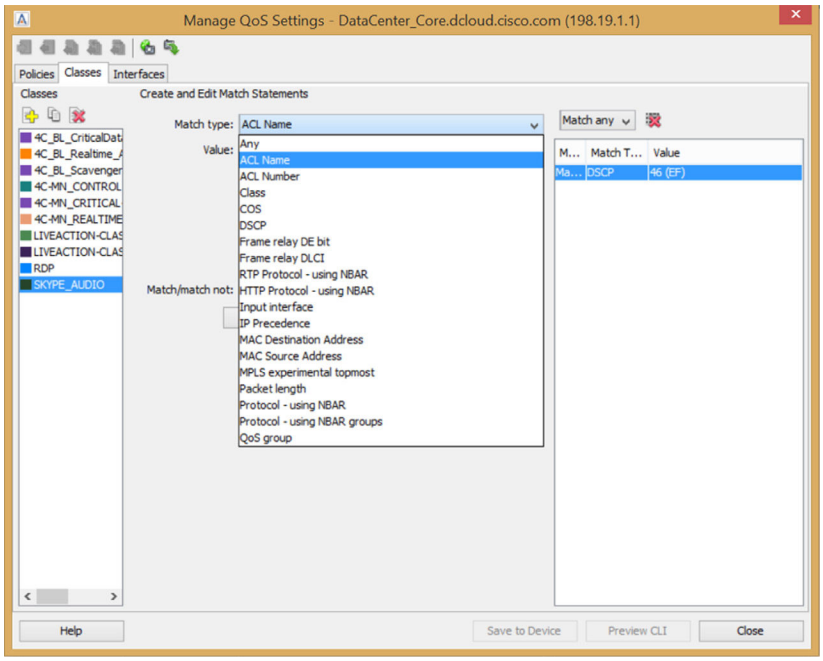


Click on the “Policies” tab to the top left of the screen to review the changes made to the SET_DSCP policy. Notice DSCP value 46(EF) is now a match type of the SKYPE_AUDIO class. This would fix this QoS issue. But what if this network has other VOIP traffic marked EF too?

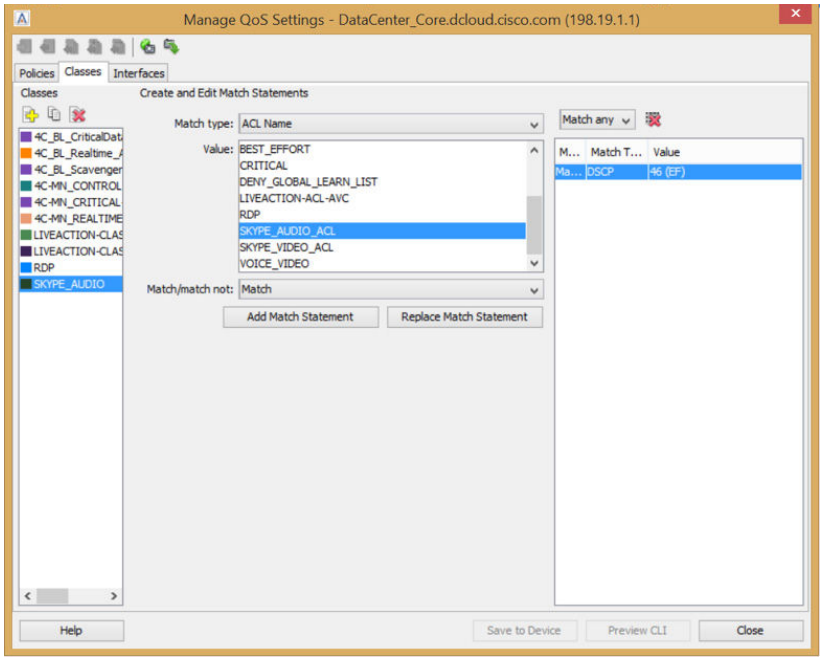
It would also match this class intended for Skype audio traffic. Since this is a classification and marking policy at the network edge, it would be best to ensure that only Skype audio matches this class. To enforce this, a second match type needs to be added to this class and the class needs to use the “Match All” setting (to use AND logic). To make these changes, click the “Edit” button.



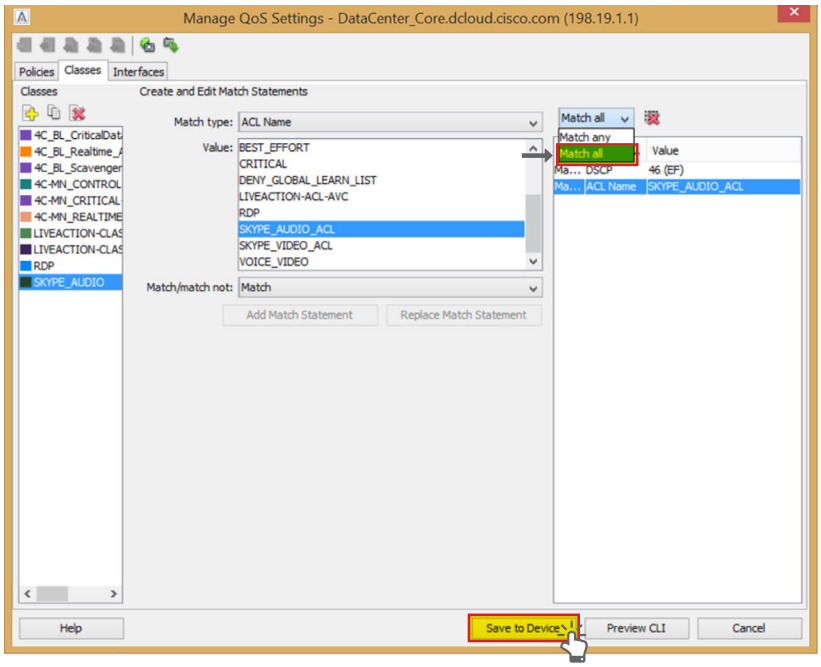
Select Match Type “ACL Name.”



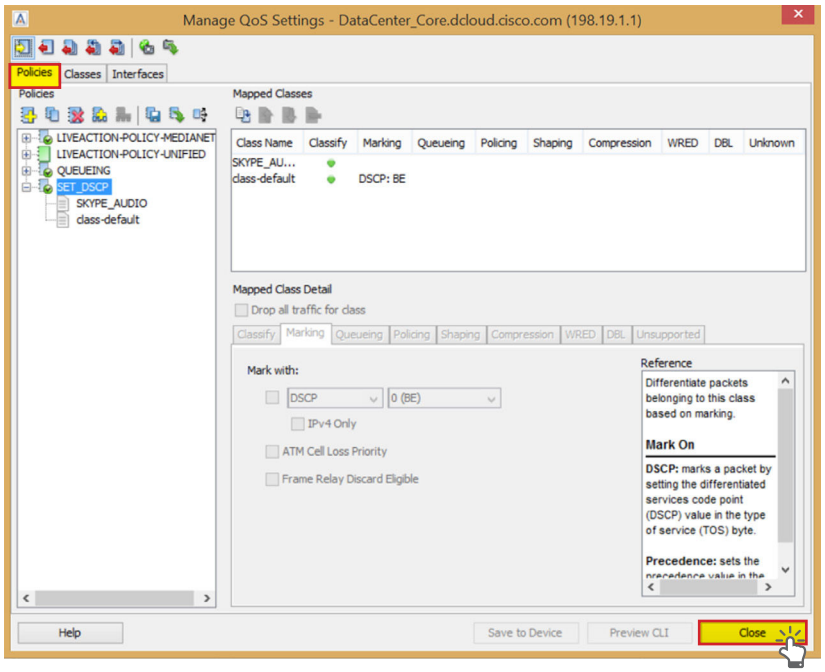
Select an access list that matches the UDP ports used for Skype client and server audio. In the example shown below, there is already an access list available called “SKYPE_AUDIO_ACL.” Select this access list and click “Add Match Statement.” See Appendix A for more information on how to create and manage access lists using LiveNX.



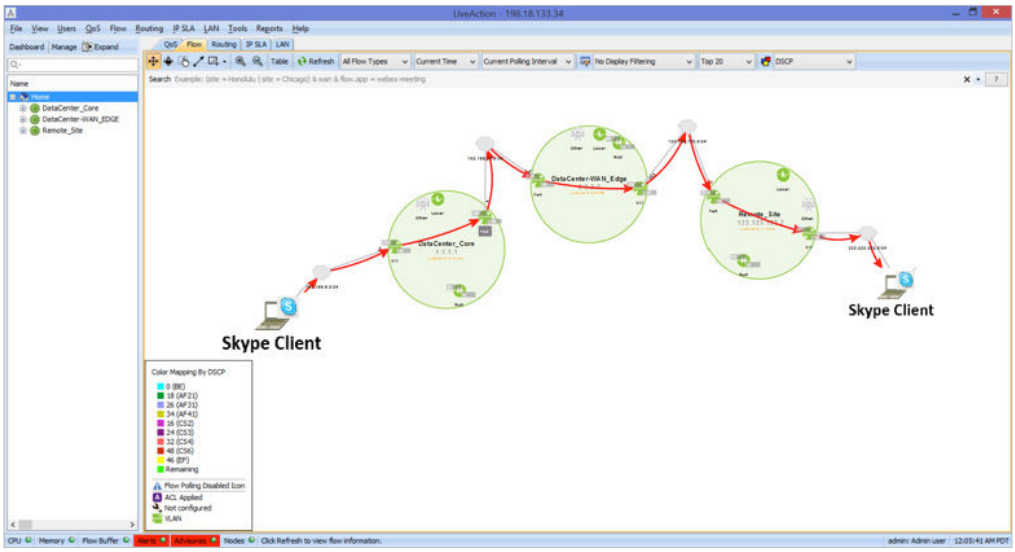
Select “Match All” from the drop-down at the top center of the screen. Click “Save To Device.”



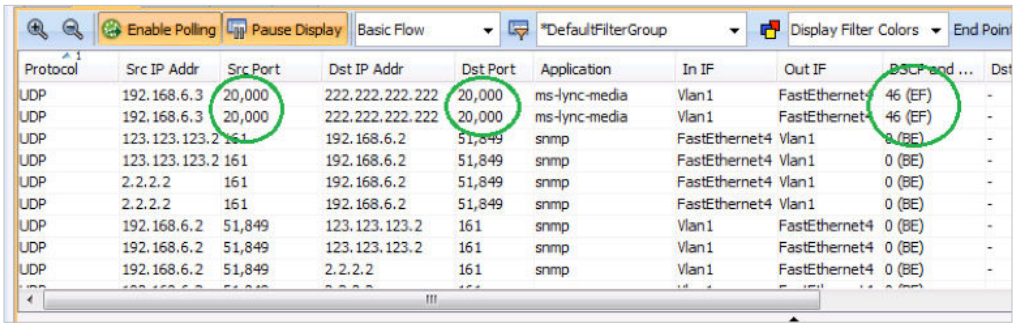
Click on the “Policies” tab to validate both match criteria and the “Match on All” is configured appropriately. If everything is valid, click “Close.”



Click “Home” in the device list to the left to return to the network diagram view. Click the “Flow” tab and click the “Refresh” button. As long as the previous example is the only network QoS issue, all arrows will now show as red for this Skype conversation. This means that all devices see Skype traffic marked with a DSCP value of 46(EF), high priority.



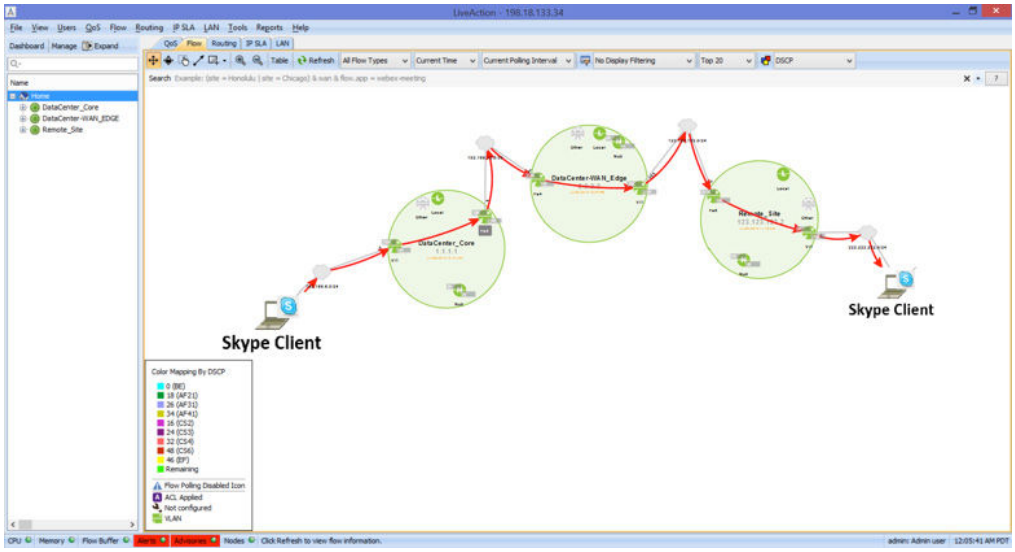
These QoS settings can be confirmed by double-clicking on any of the devices that show red arrows painted through them. In the LiveNX real-time NetFlow view below, the UDP ports are in the appropriate range and the DSCP value is EF.



Note that this QoS classifying and marking example provided is very simple. The steps shown need to be repeated throughout the network environment to ensure all Skype client and server audio DSCP markings are honored appropriately.

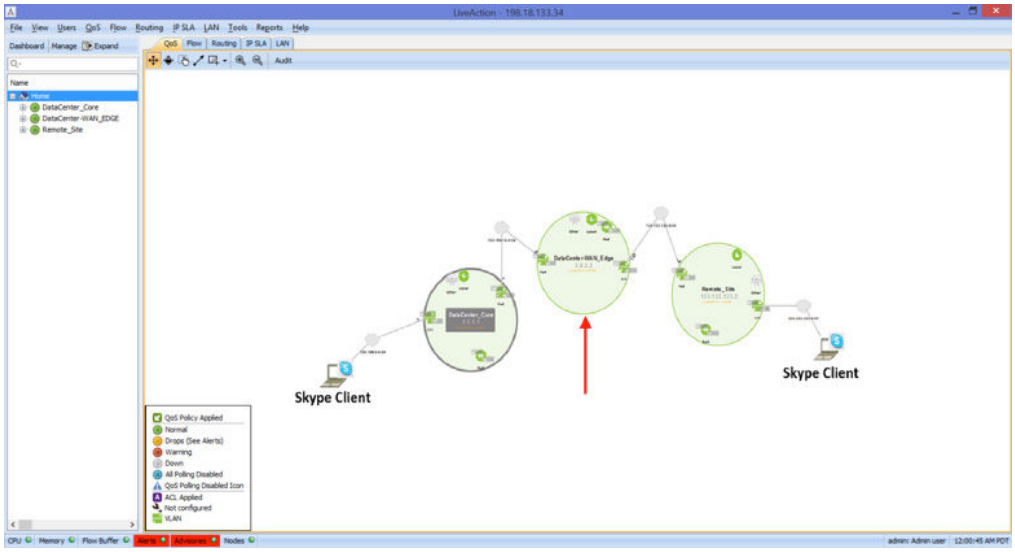
Microsoft Skype Audio QoS Queuing with LiveNX

Once Skype audio traffic has been classified and honored as high priority (DSCP 46(EF)) end-to-end in the network, steps should be taken to ensure Skype traffic is prioritized appropriately. The diagram below shows Skype traffic being marked appropriately (as red) end-to-end.

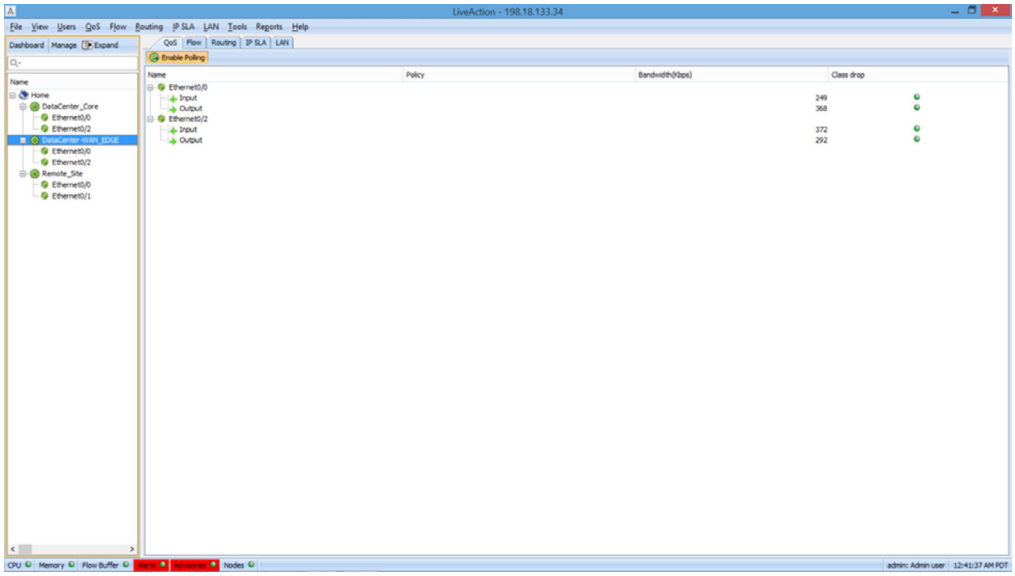


This prioritization needs to happen at any congestion point in the network. Congestion occurs most often at the WAN edge, but can also happen in the LAN. When implementing a QoS queuing policies, start where the problem occurs most, the WAN edge. The following pages will show how to configure a queuing policy using LiveNX to prioritize Skype traffic at the WAN edge.

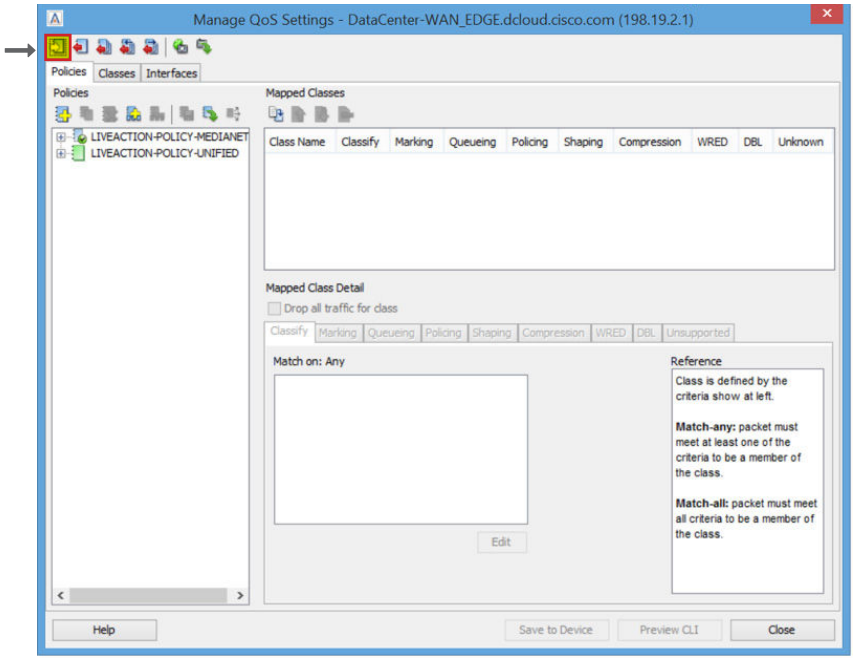
First, click the “QoS” tab and then double-click the middle device (in this example the data center WAN edge device).



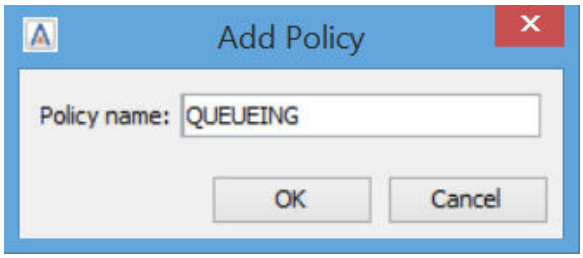
This brings up a list of the interfaces on this device. In this example, there are no QoS polices applied to any interface. To create a queuing policy, right-click on an interface and go to QoS > Manage QoS Settings.



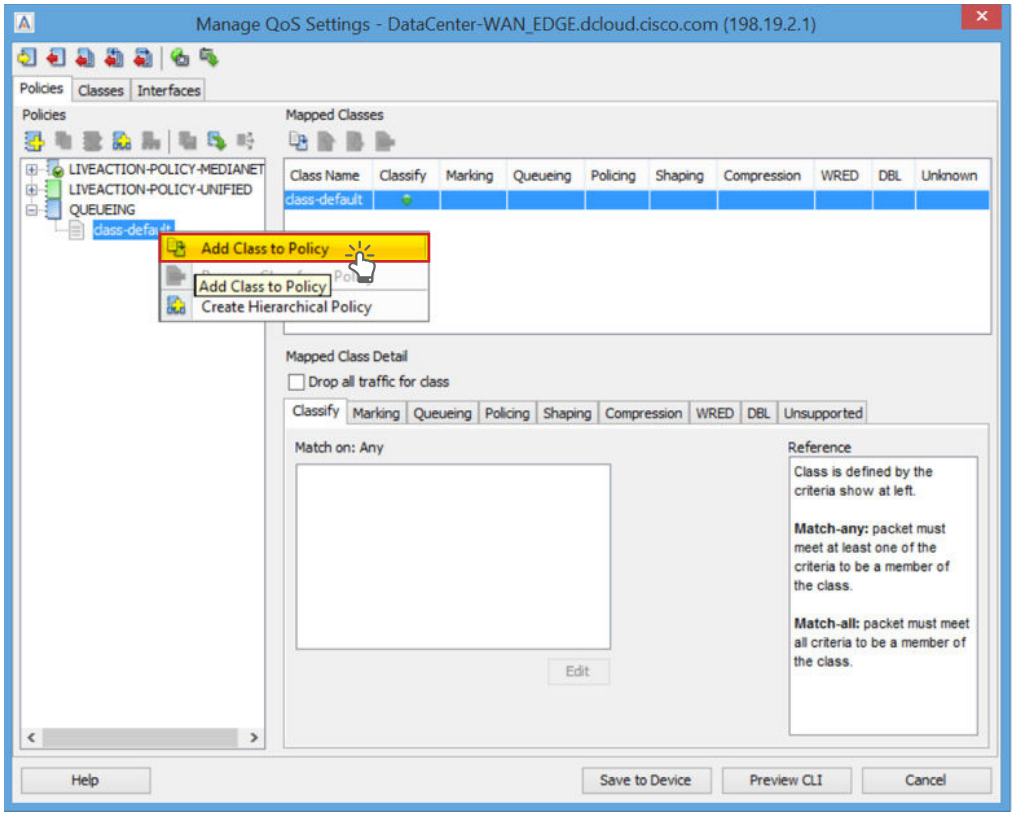
This brings up the Manage QoS Settings window, as seen below. To create a new policy, click the “Add Policy Button” at the top left of the page.

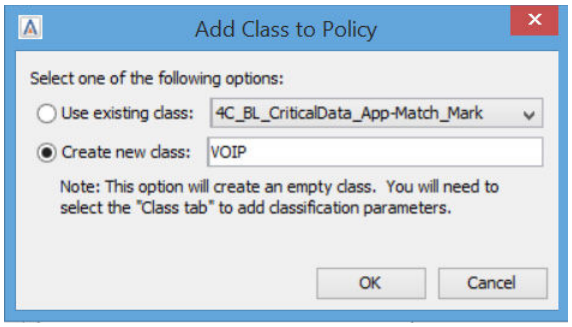


In this example, the new policy will be named QUEUEING.

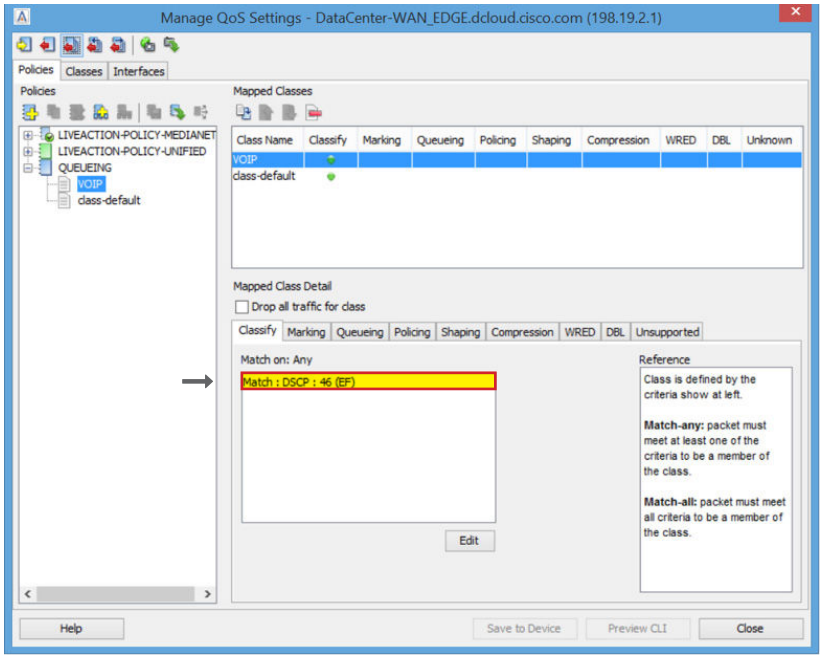


Right-click on the policy and add a new class to the policy. This new class will be called VOIP.

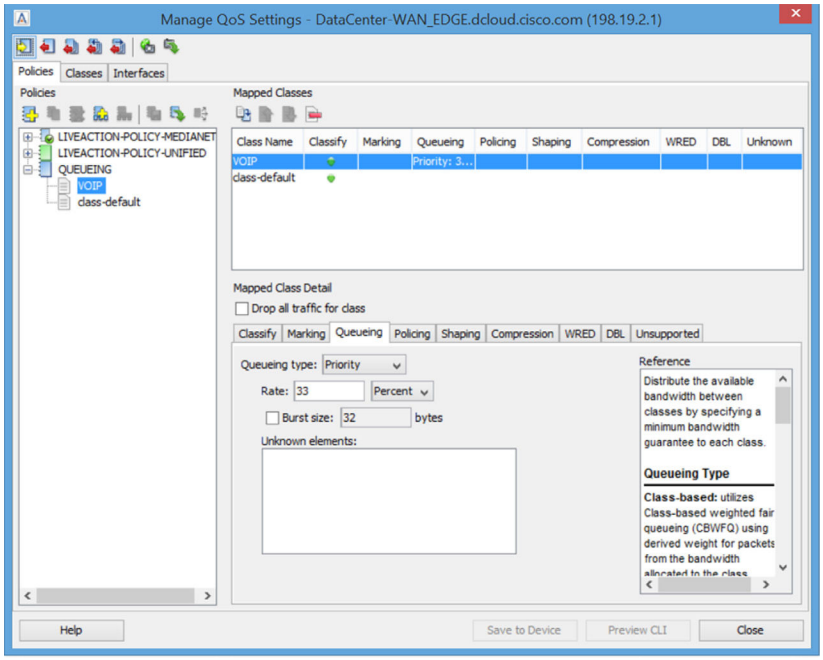




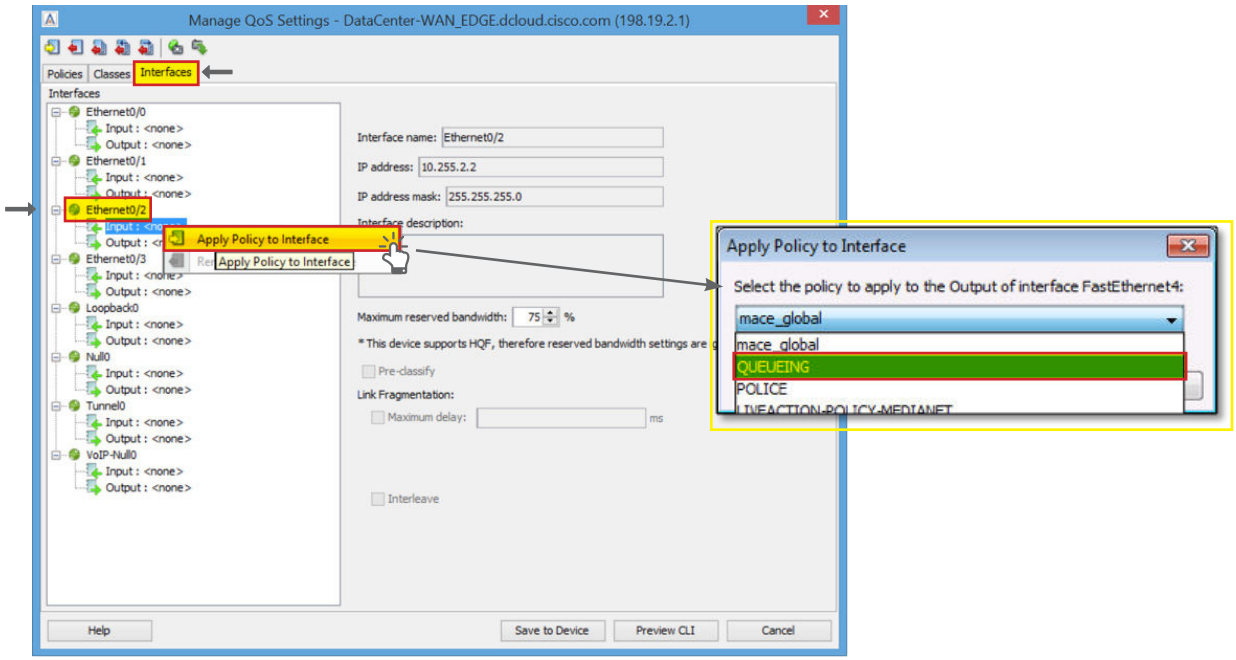
Add match criteria as described above to match EF to the VOIP class.



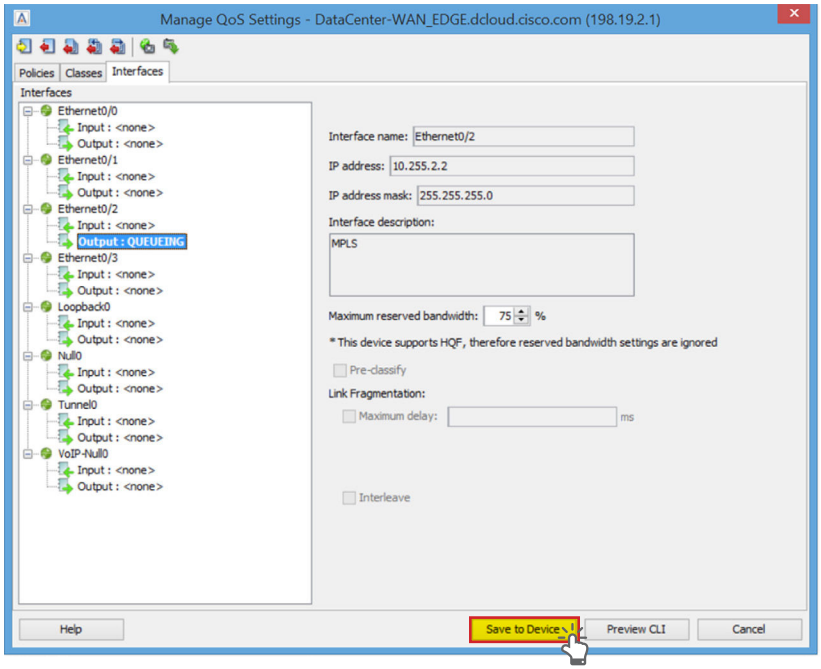
Click the queuing tab and select the queuing type “Priority.” Set the bandwidth percentage to 33%. This is a safe starting number for this queue and can be adjusted by monitoring the queues performance over time. See below for examples of how to monitor this queue.



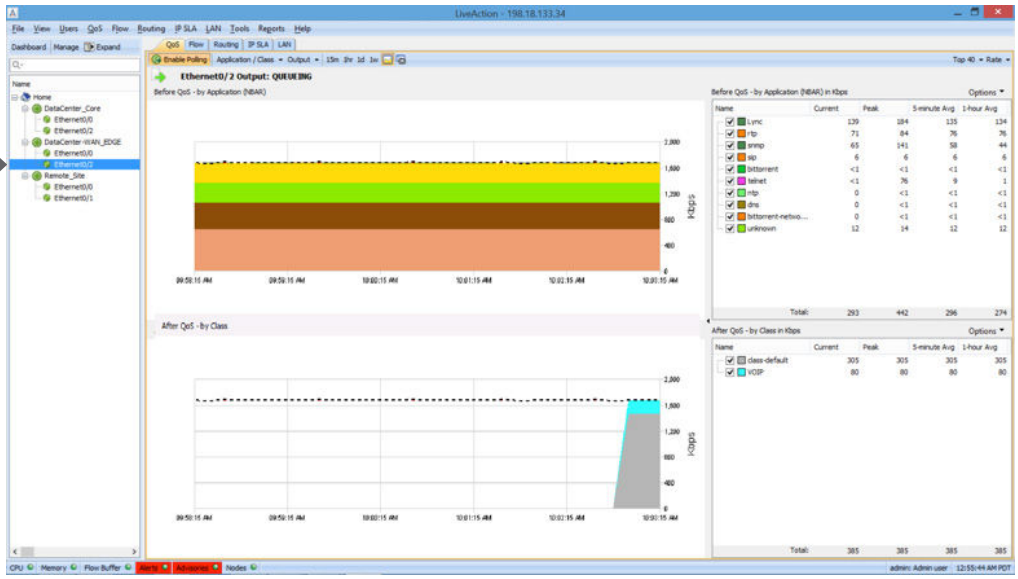
Click on the “Interface” tab, right-click on the output of interface Ethernet 0/2 (the WAN interface) and apply the QUEUING policy.



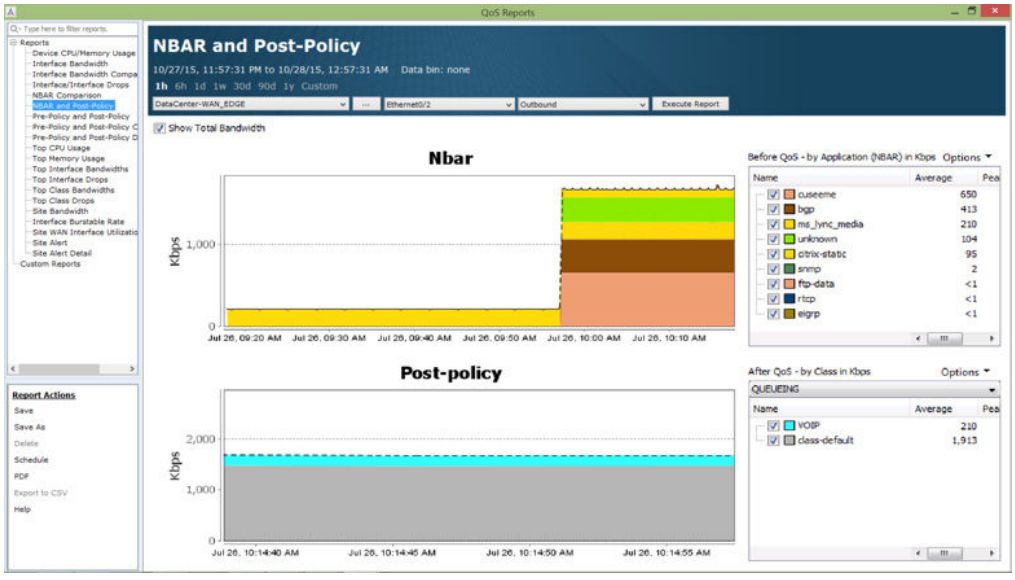
Click “Save to Device” and “Close.” Skype audio traffic will now be given priority treatment when this WAN interface becomes congested.



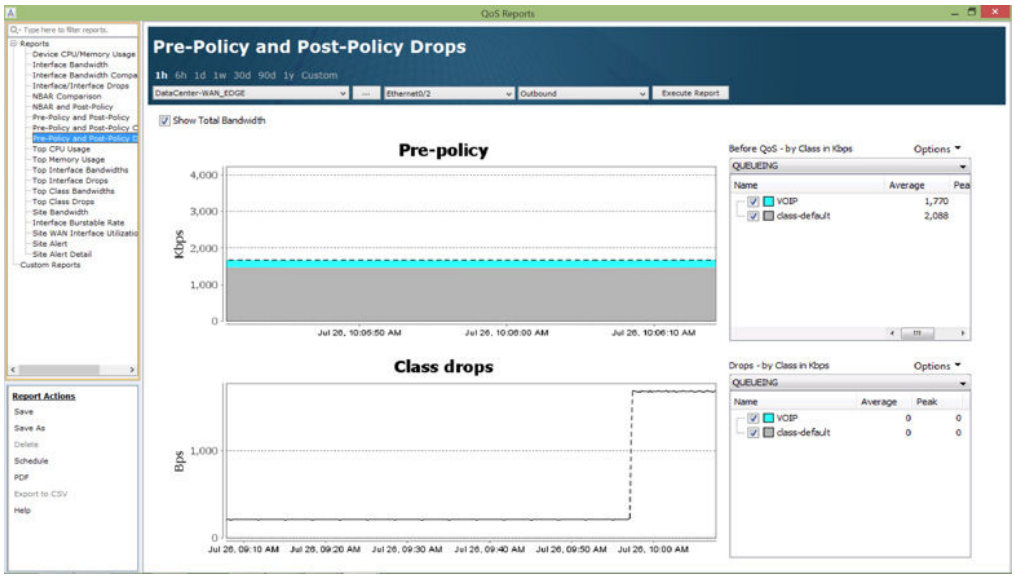
To verify Skype's performance return to the network diagram, click the "Home" icon at the top left of the screen, then select the "QoS" tab, and double-click on the Ethernet 0/2 interface. The graph and legend to the bottom of the screen shows the real-time performance statistics of this new QoS policy. This screenshot confirms that 46(EF) traffic (Skype in this example) is being protected by the VOIP queue.



To see this same information historically click the "1hr" button to the top of the screen to run a historical report for this policy's performance. Click the "Custom" button to view this policy for an administratively defined time range. In the historical report shown below, notice how the "Post-Policy Report" shows traffic in the VOIP queue (Skype in this example) at 210kbps. This matches with the real-time report above.



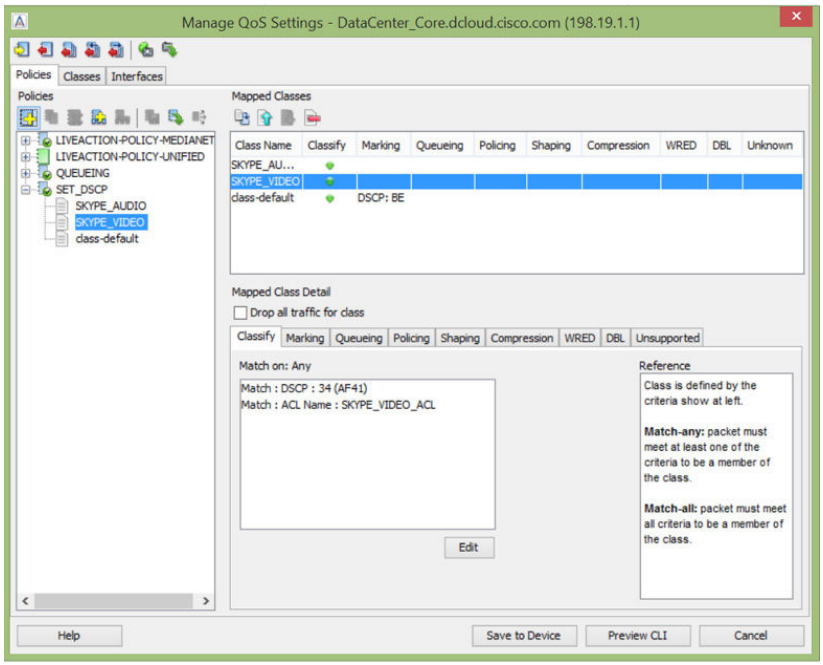
Another QoS historical report that is useful for monitoring QoS performance is the “Pre-Policy and Post-Policy Drops” Report. The “Class drops” graph and legend will show, which queues have been dropping any traffic. In this example there are no drops in the VOIP queue, this validates that Skype traffic is performing optimally on this interface for the time range shown.



Microsoft Skype Video QoS with LiveNX

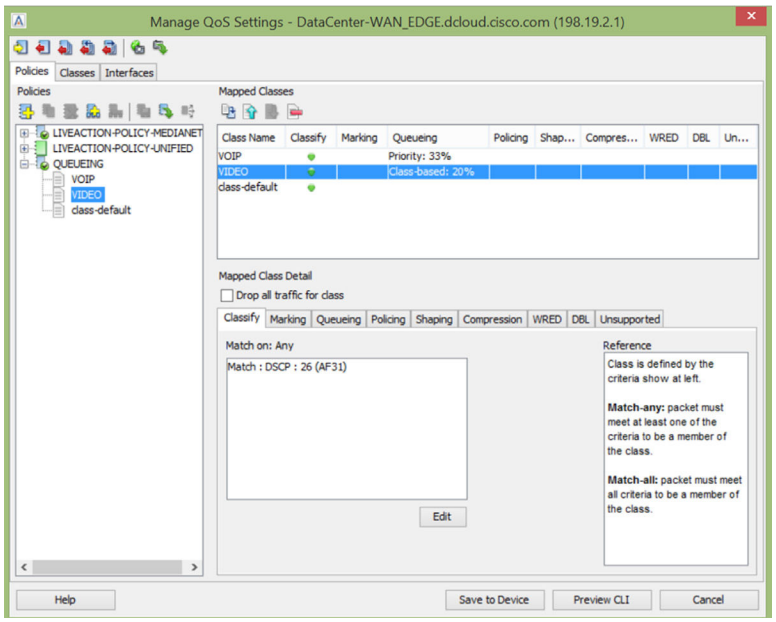
The steps to configure and confirm Skype video application performance are very similar to the steps shown for Skype audio. The task required will be summarized below.

First, ensure Skype video is classified and matched appropriately. This would include ensuring Skype video traffic is trusted as it enters the network edge. Using the example from the Skype audio section of this document, add a “SKYPE_VIDEO” class to the SET_DSCP policy. It is recommended to use “Match on ALL” for both the DSCP value and ACL to ensure only Skype traffic matches this class.

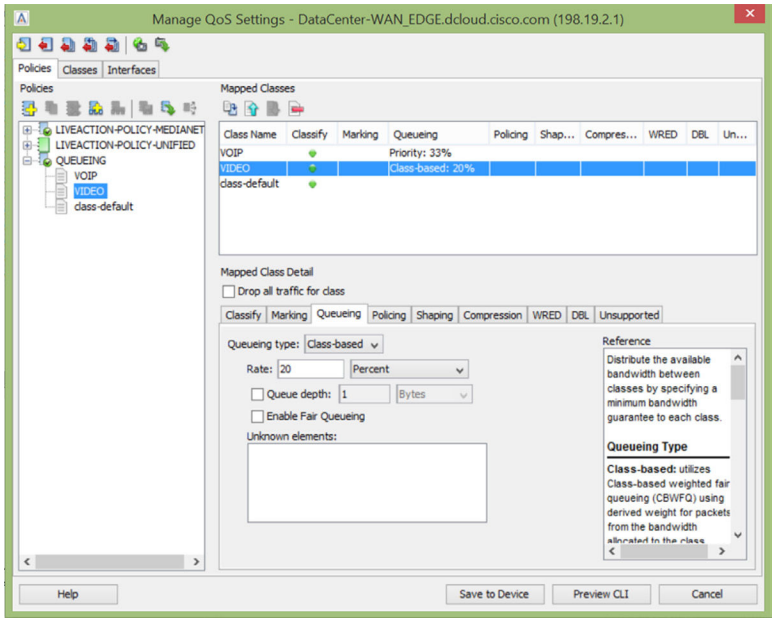


Once the appropriate trust configuration is in place, LiveNX will validate that the DSCP value is marked end-to-end by showing the colored arrows across the network map. In the example below, the red arrows indicate Skype audio (EF) and the gold arrows indicate Skype video (AF41).

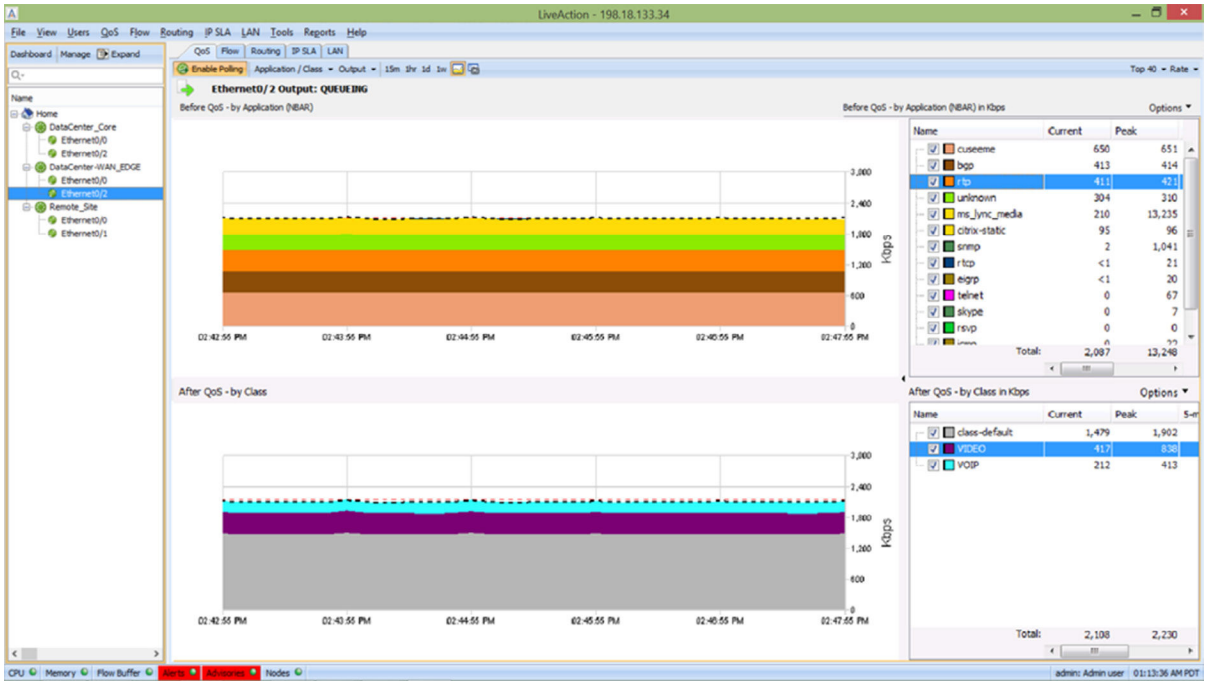
Once DSCP markings are confirmed to be honored through the network end-to-end, Skype video should be prioritized on the appropriate network devices. Using LiveNX's QoS tools, create a new video class on the same queuing policy that was created for Skype audio. Configure the class to match on DSCP 34(AF41).



Configure this VIDEO class to queue traffic. In this example, the video class will be assigned 20% as a CBWFQ.



Once the video queue is created, its operation can be confirmed by viewing the interface's QoS statistic. In the example, below, video traffic is being matched in the bottom graph in purple.



APPENDICES:

Appendix A: **LiveNX ACL Management for Skype**

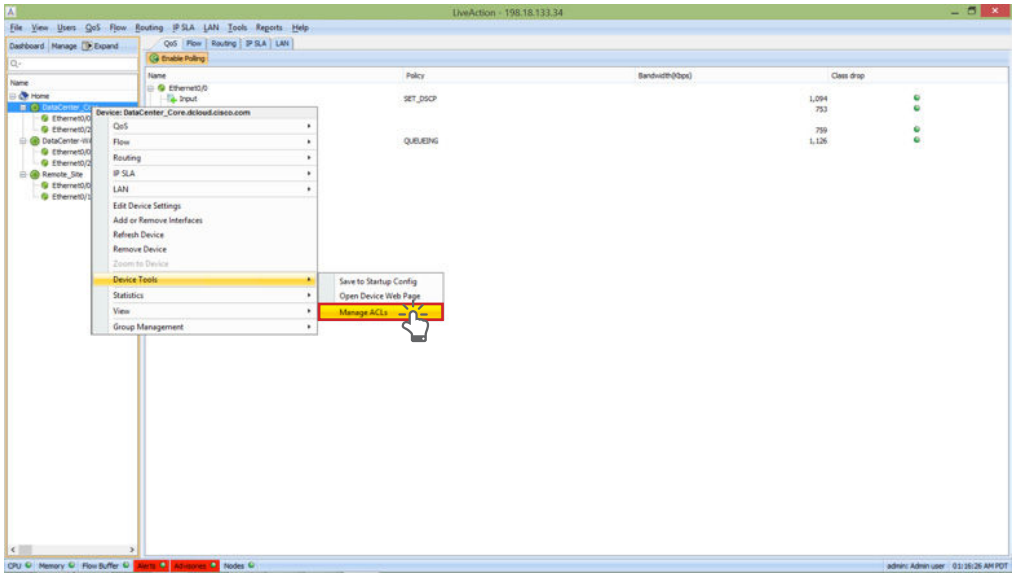
Appendix B: **Skype with Cisco Performance Monitoring**

Appendix C: **Skype QoS Audio Configuration Using NBAR2 Definitions**

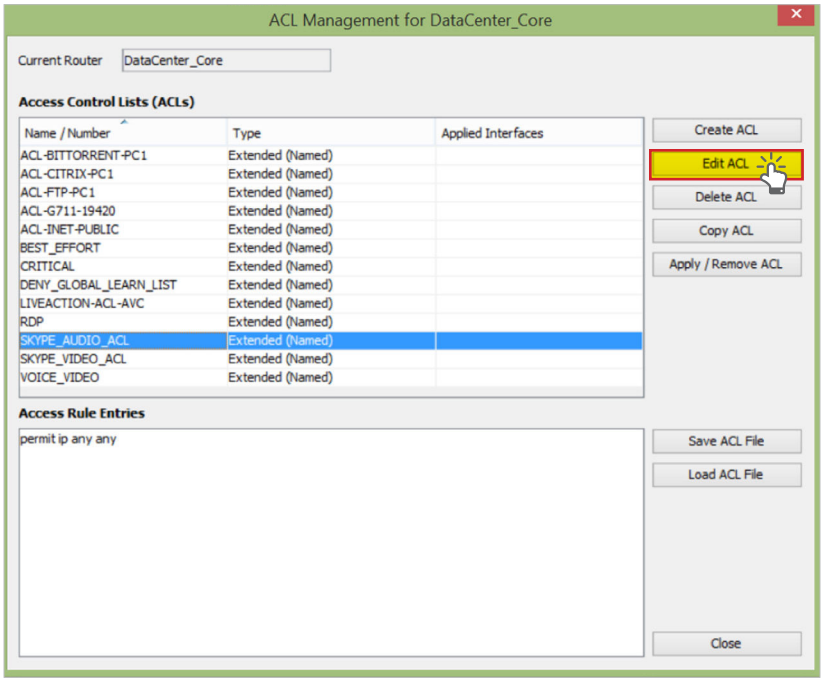
Appendix D: **Skype QoS Queuing with LiveNX and NBAR2**

APPENDIX A: LIVENX ACL MANAGEMENT FOR SKYPE

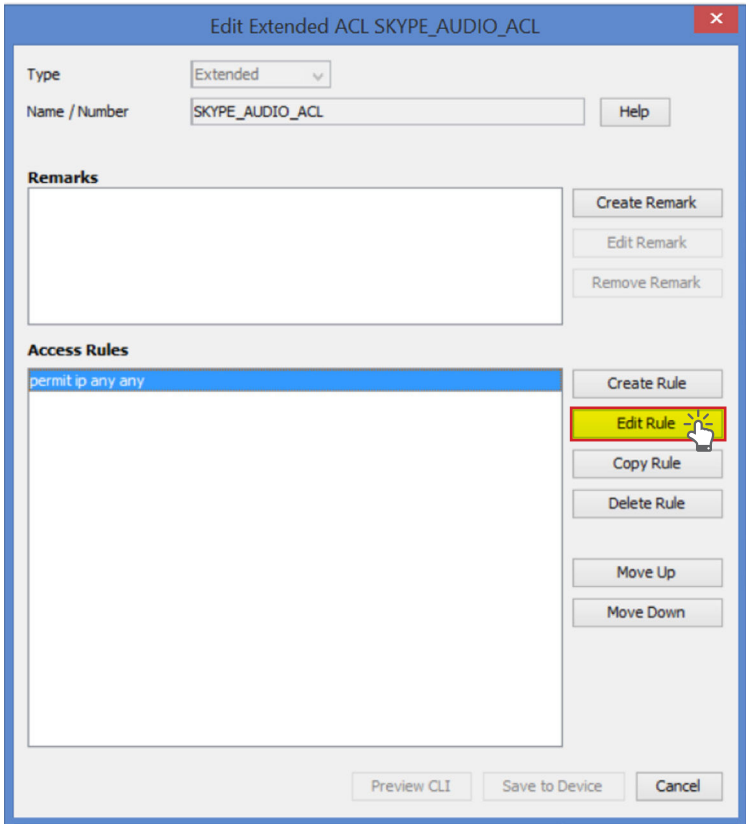
LiveNX has ACL management capabilities that allow administrators to configure and push access lists to the enterprise. This gives engineers the ability to centrally manage and deploy ACL in their network. To manage the access list on a device, right-click on the device, select “Device Tools,” and “Manage ACLs.”



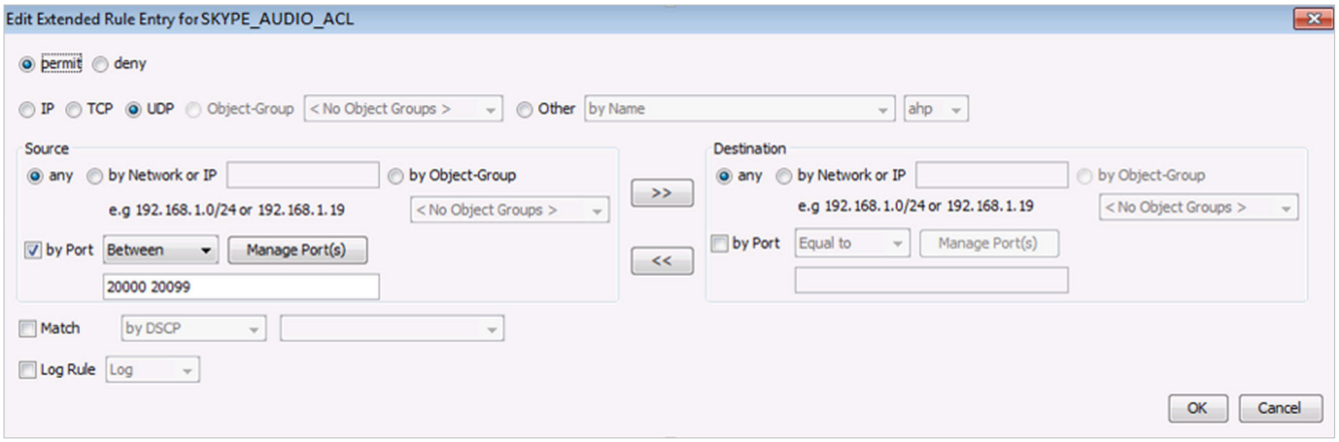
A list of the ACLs found on the device will appear. Click on one of the access lists to see its configuration at the bottom of the screen. Click the “Edit ACL” button to manage the access list. The example ACL below shows the information that would match Skype Audio in this document.



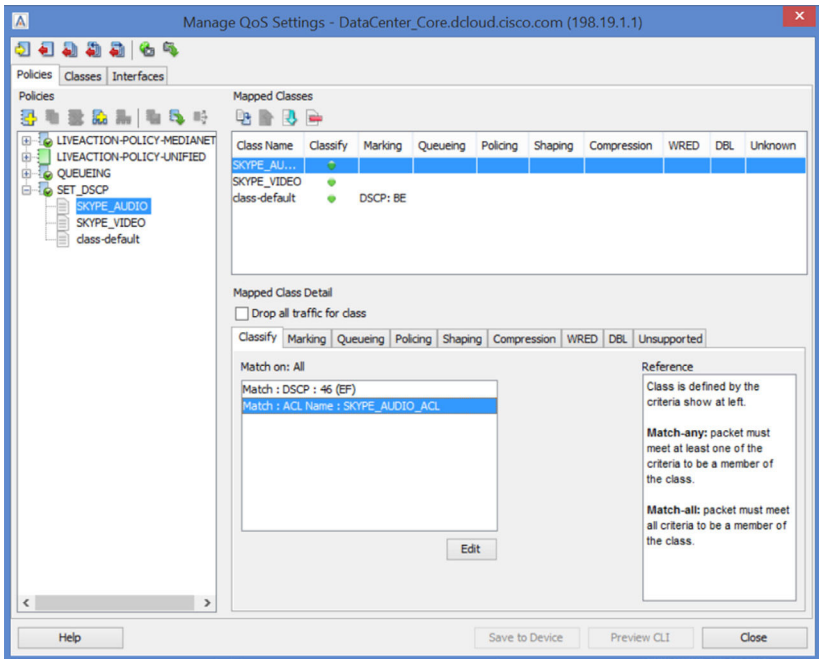
Select one of the ACL rules and click “Edit Rule” to update the variables as appropriate.



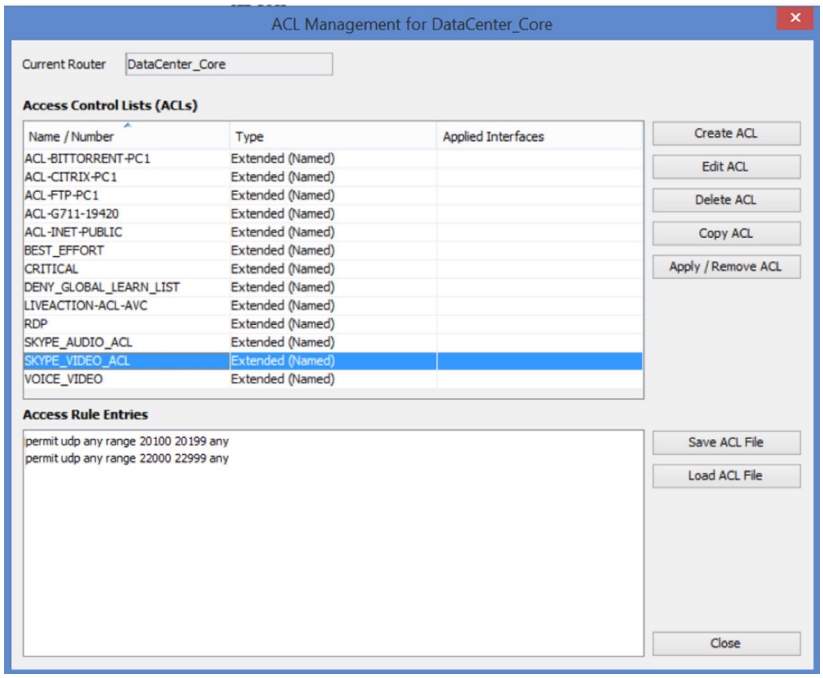
Edit the ACL as requited and click “OK” when finished.



The ACL referenced above can be used as the match criteria for a QoS policy (as shown below).



Below is another example ACL. This example shows the information that would match Skype video in this document.

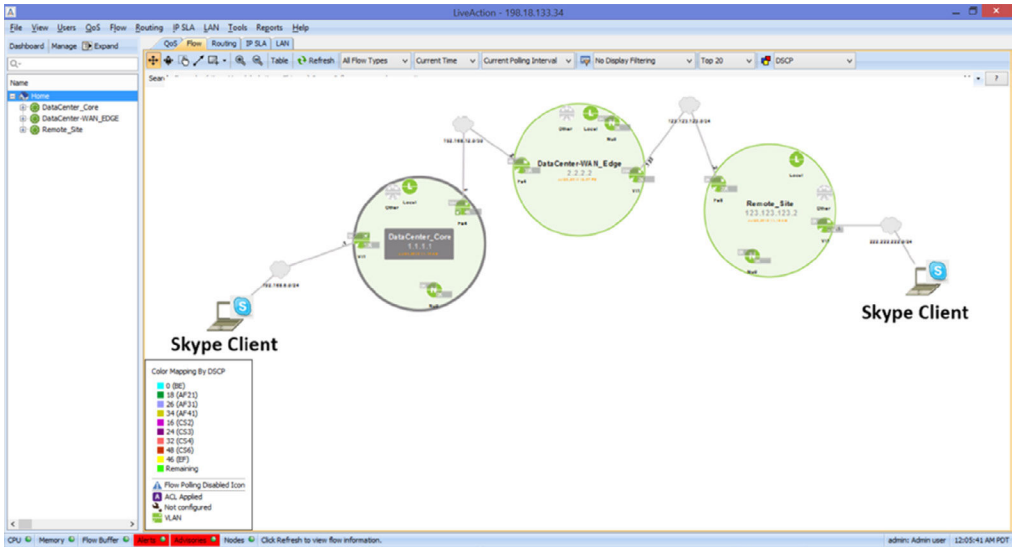


APPENDIX B: SKYPE WITH CISCO PERFORMANCE MONITORING

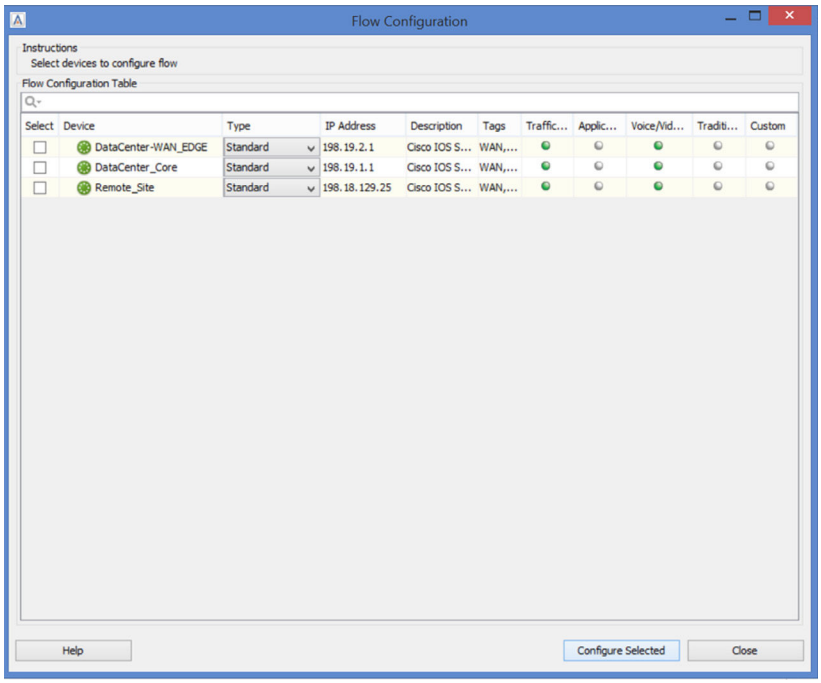
LiveNX supports the Cisco Performance Monitoring Flexible NetFlow template. This will allow administrators to deploy and manage Performance Monitoring in the network infrastructure and gather application performance metrics (packet loss, jitter) for voice and video over IP. This advancement in technology gives administrators the ability to understand how these applications are performing without the use of probes or other costly network appliances. Using the technology now embedded inside Cisco network equipment, voice and video call quality issues can be detected and reported to network administrators before end-users ever complain.

The first step in gaining this visibility into voice and video application performance is to enable this flow type in the Cisco network infrastructure. LiveNX can automate these tasks and enable the deployment of this complex set of configurations in a simple point-and-click manner. This can be done with the following step:

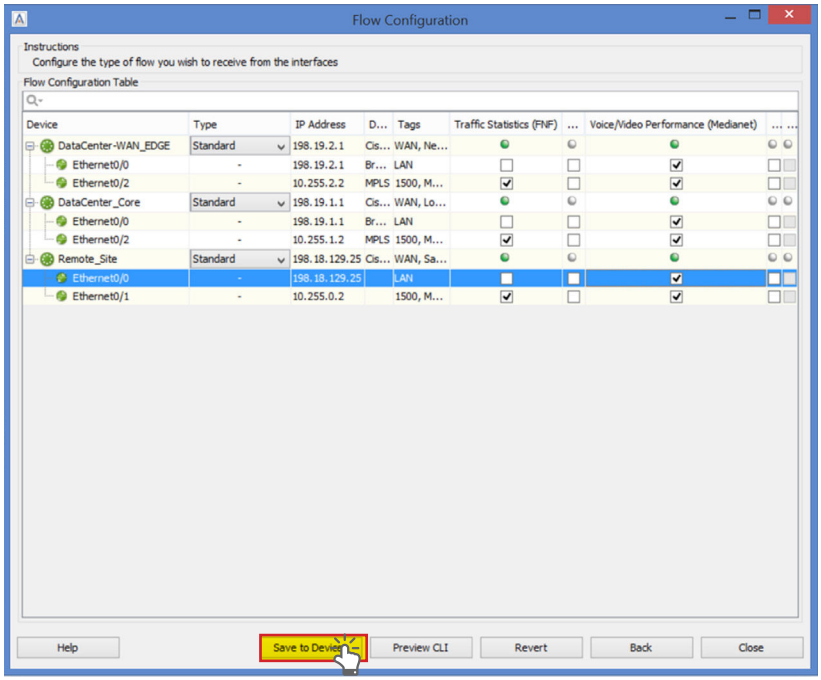
From the Menu bar, Select Flow > Configure Flow.



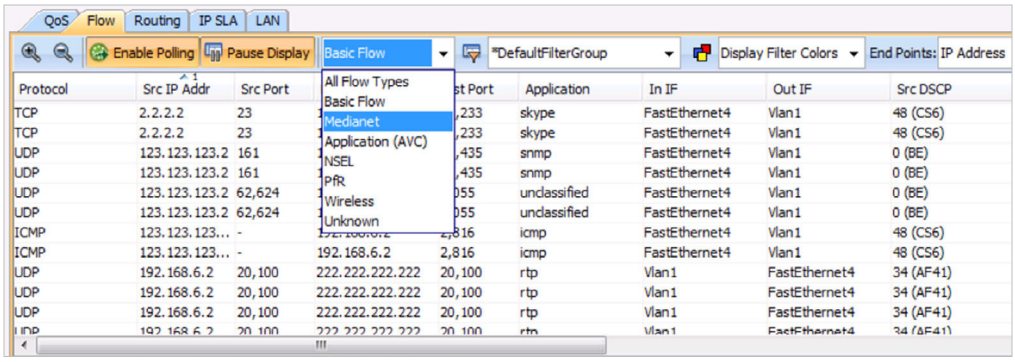
Check the devices to enable the Voice/Video Performance (Medianet) flow type and click “Configure Selected.” In this example, all three devices are checked.



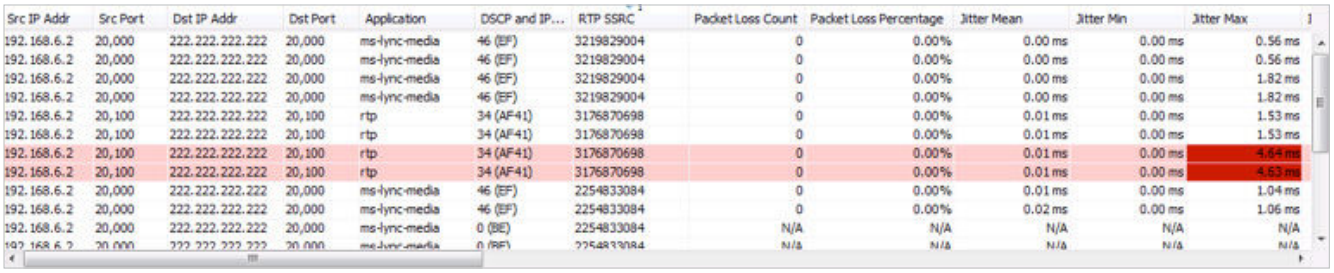
Check the box of the desired technology on each interface and click “Save to Devices.” In this example, all interfaces have FNF (basic Flexible NetFlow) and Voice/Video Performance (Medianet) selected.



Once the Performance Monitoring flow type is enabled, navigate to a device's real-time NetFlow view by clicking the "Flow" tab and then double-clicking on a device in the network map. Select the flow type drop down menu and select "Medianet."



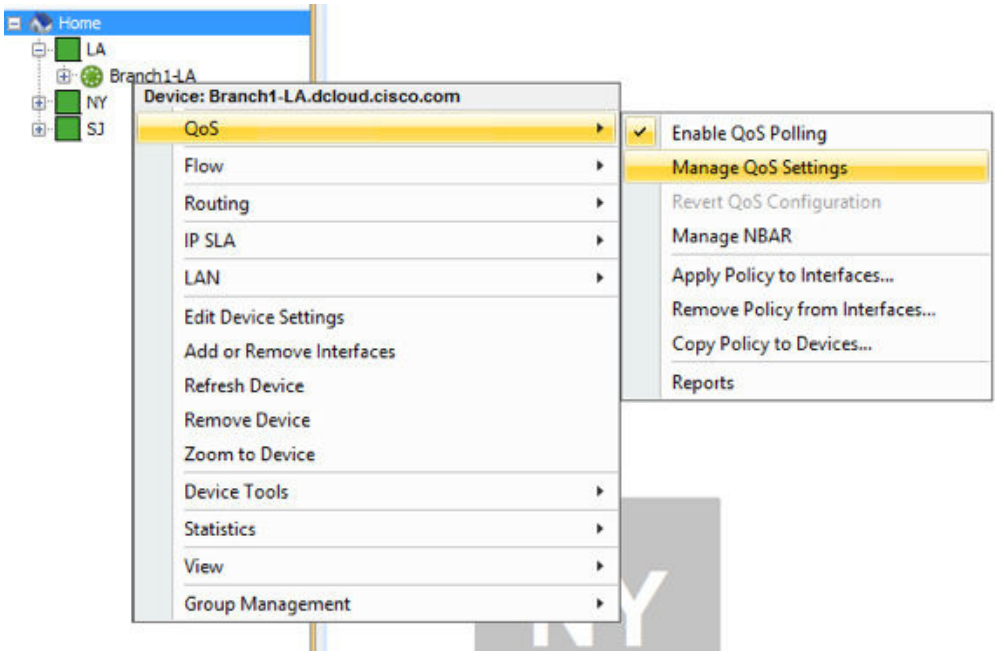
The real-time Performance Monitoring flow records will now appear. Packet loss and jitter measurements will now be visible in the flow record. In the example below, two of the flows are being highlighted in pink due to an alarm being triggered by the cells in red. In this example, these flows Jitter Max measurements triggered an alarm. Network administrators are able to receive this performance alert via email or syslog message.



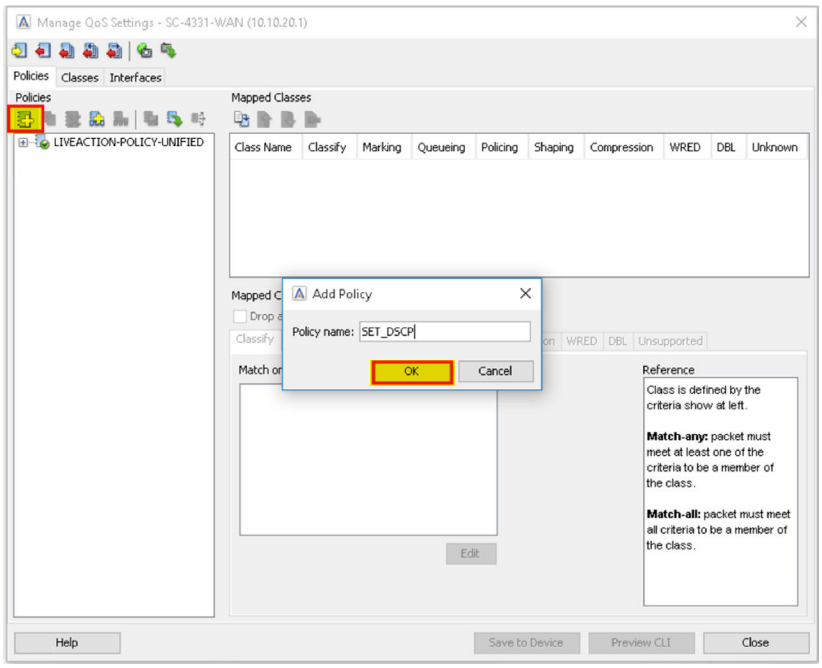
APPENDIX C: SKYPE QOS AUDIO CONFIGURATION USING NBAR2 DEFINITIONS

LiveNX and NBAR2 makes protecting Skype traffic extremely easy. Earlier in this guide, methods were described on how to recognize and mark ingress traffic using ACL's to identify ports used for Skype audio or video. This required changes to the Microsoft servers and clients. With NBAR2 protocol pack 12 (or higher) that is no longer necessary. NBAR2 applications can be applied directly to QoS polices using the LiveNX QoS Management GUI.

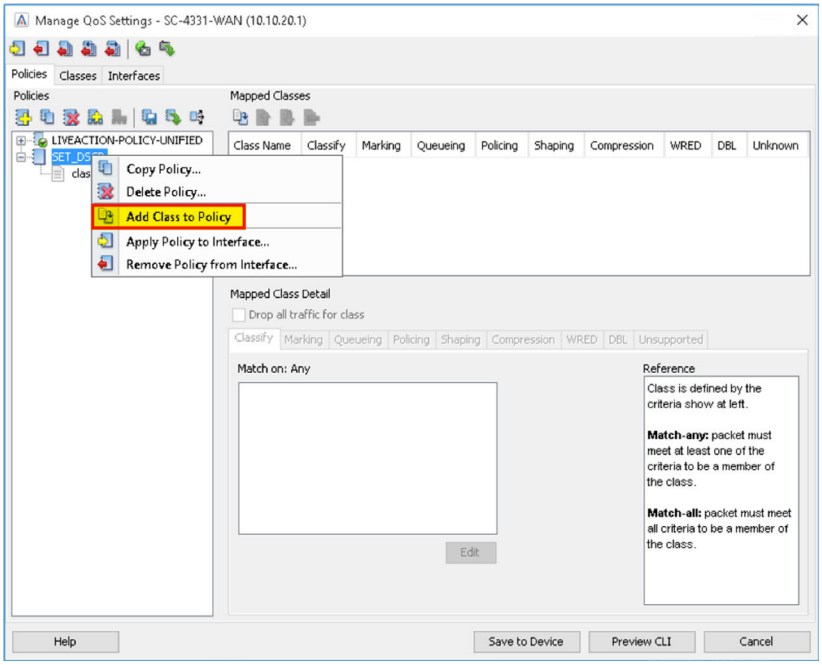
Begin by creating an ingress to QoS Policy to Classify Skype Audio as DSCP 46. To do this, open the LiveNX Manage QoS Settings window.



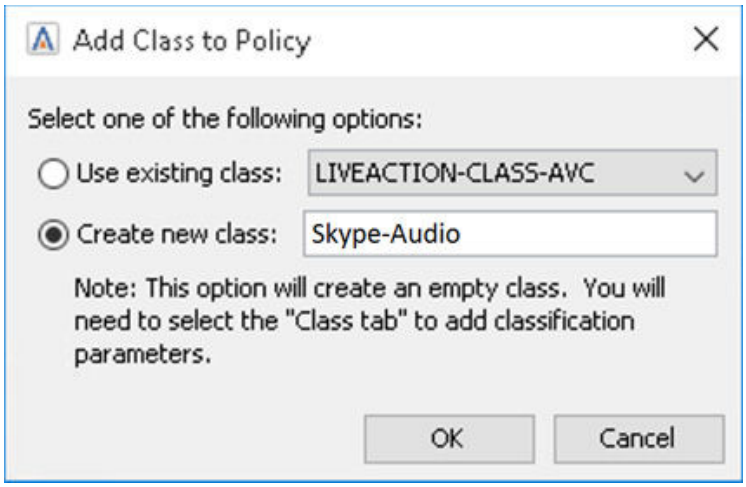
Create a new QoS Policy by selecting “Add Policy” and give the policy a name.



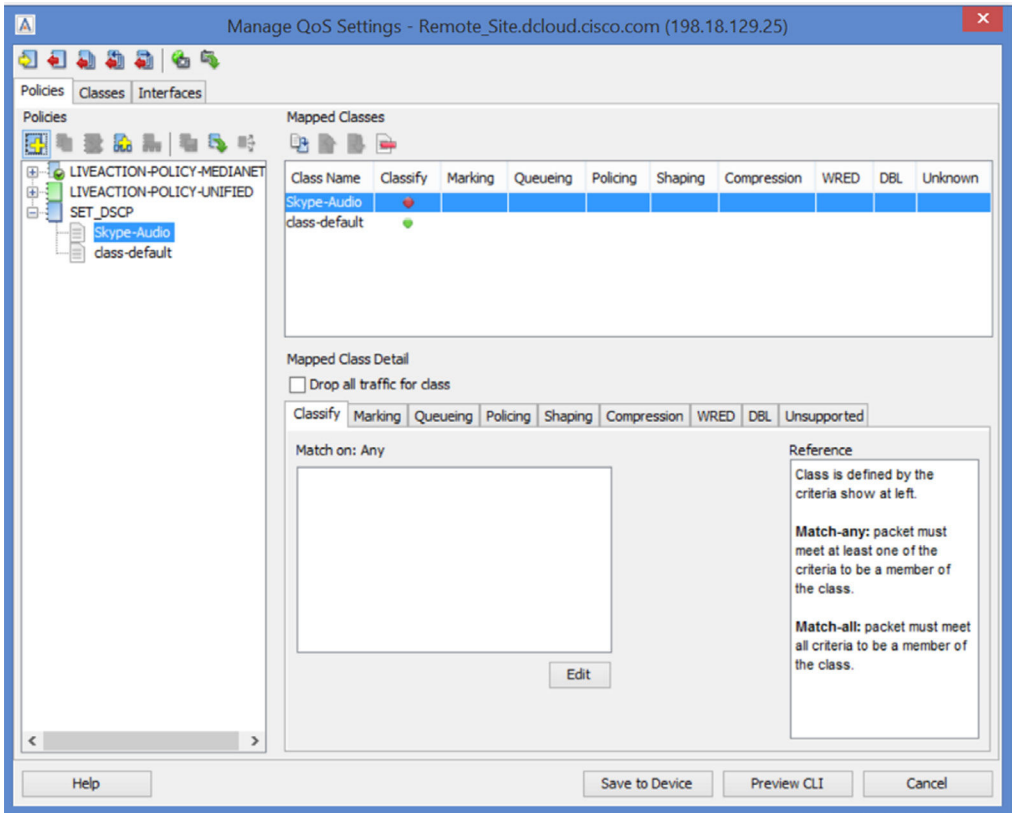
After creating the new policy, right click on the new policy and select “Add Class to Policy.”



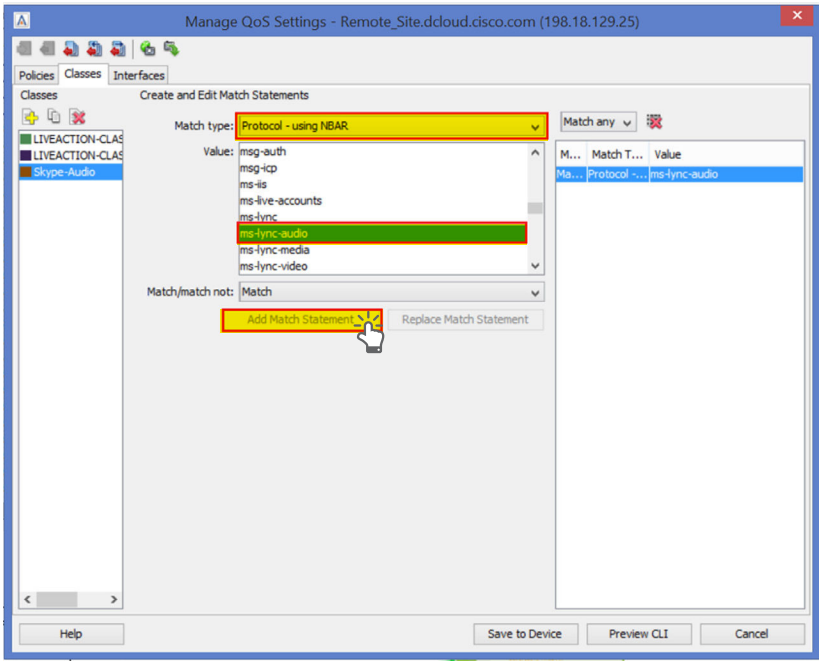
Give the new class a name.



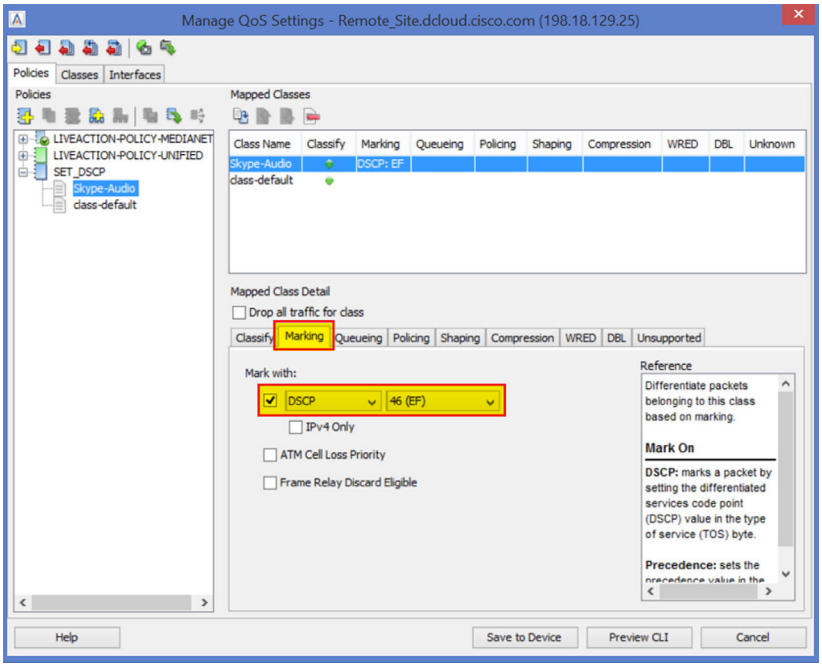
Next, select “Edit” to add Skype audio to the class.



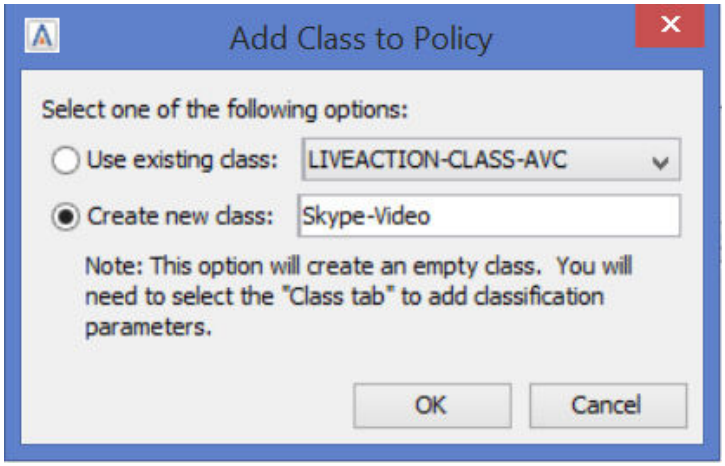
On the Class Tab, select “Protocol–using NBAR” as the match type. Then select “ms-lync-audio” as the NBAR application, and then select “Add Match Statement.”



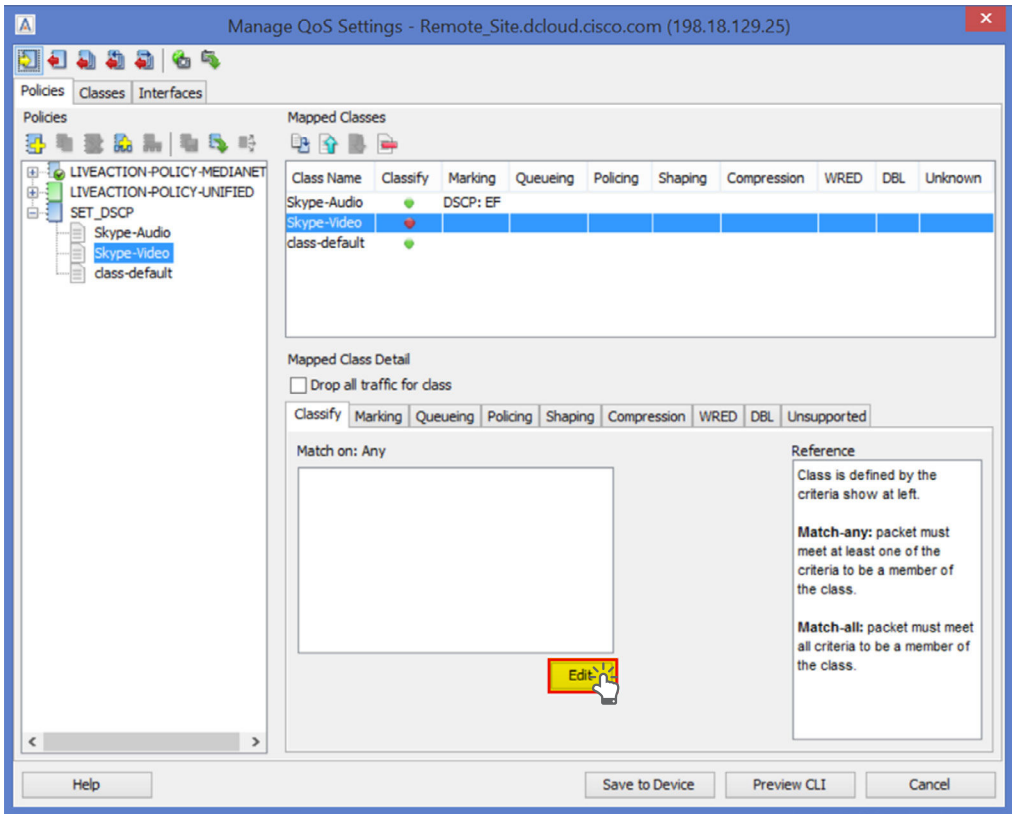
Now, go back to the Policies tab, and then select the Marking tab. On the Marking tab check the box for DSCP and select “46 (EF).”



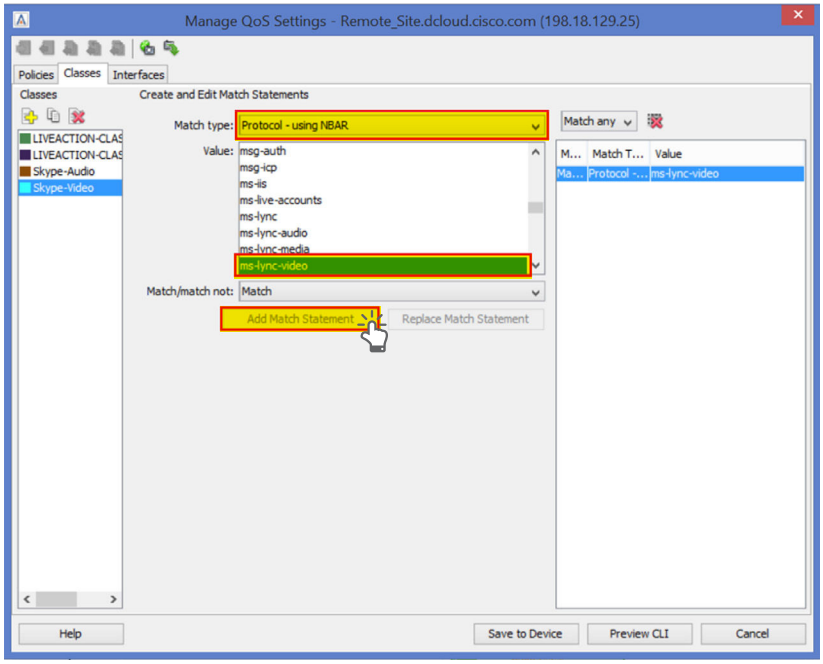
Now add another “class” to the SET_DSCP policy to mark our Skype video traffic as DSCP 34.



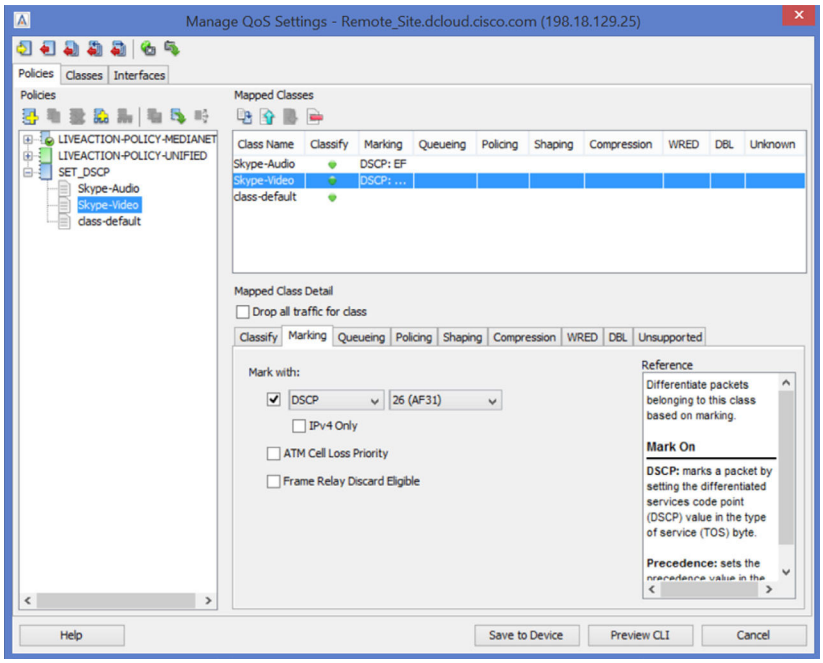
After creating the new class please select “Edit.”



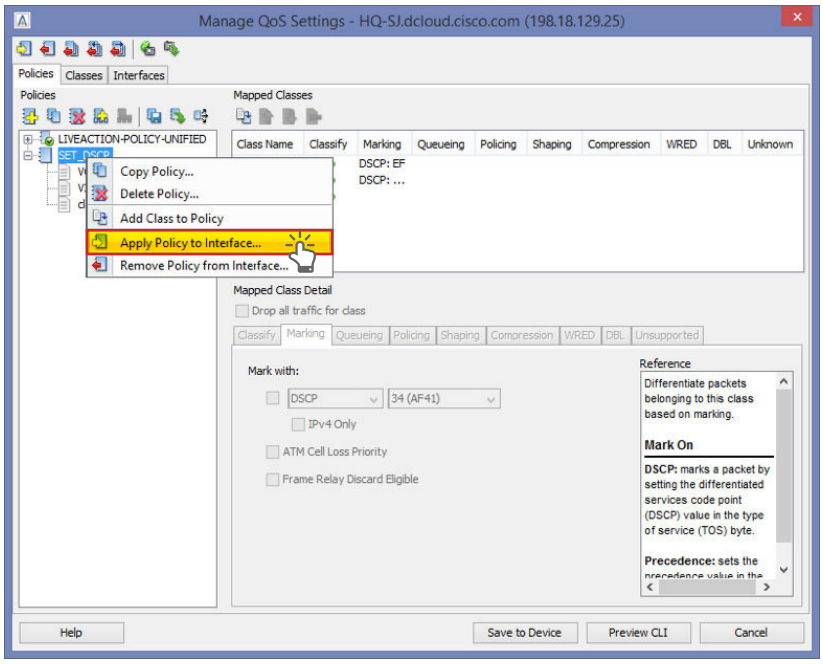
Once on the class tab please select the match type to be “Protocol–using NBAR” and then select “ms-lync-video” and lastly “Add Match Statement.”



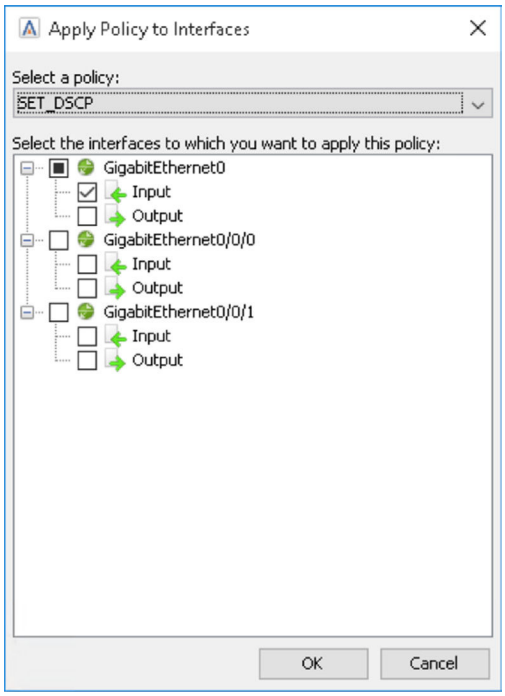
Go back to the “Policies Tab” and select the “Marking Tab” to properly mark Skype video as DSCP 34.



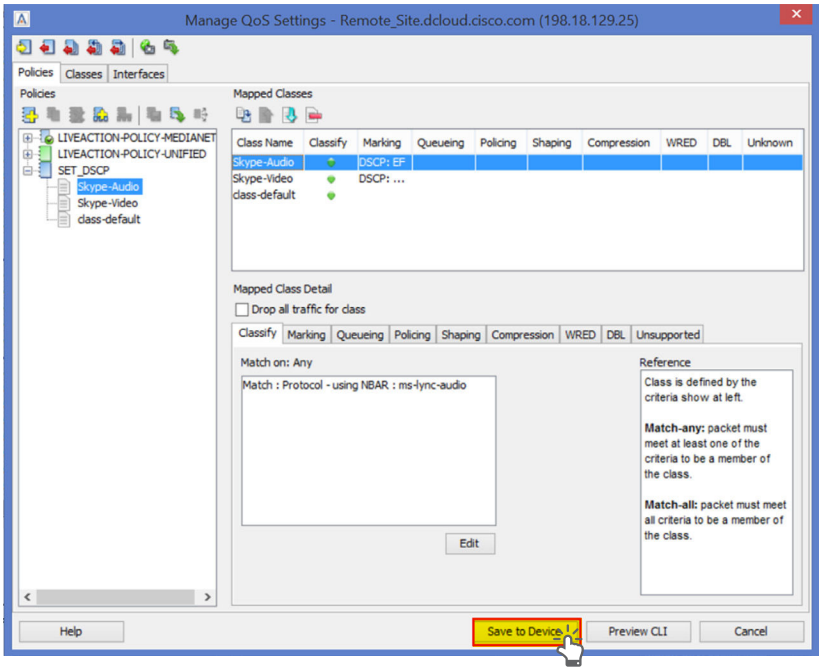
Now with a policy to identify and mark the Skype audio and video, apply the new policy to an interface by right-clicking on the policy and selecting “Apply Policy to Interface.”



Select the interface to apply the policy to and select “OK.”



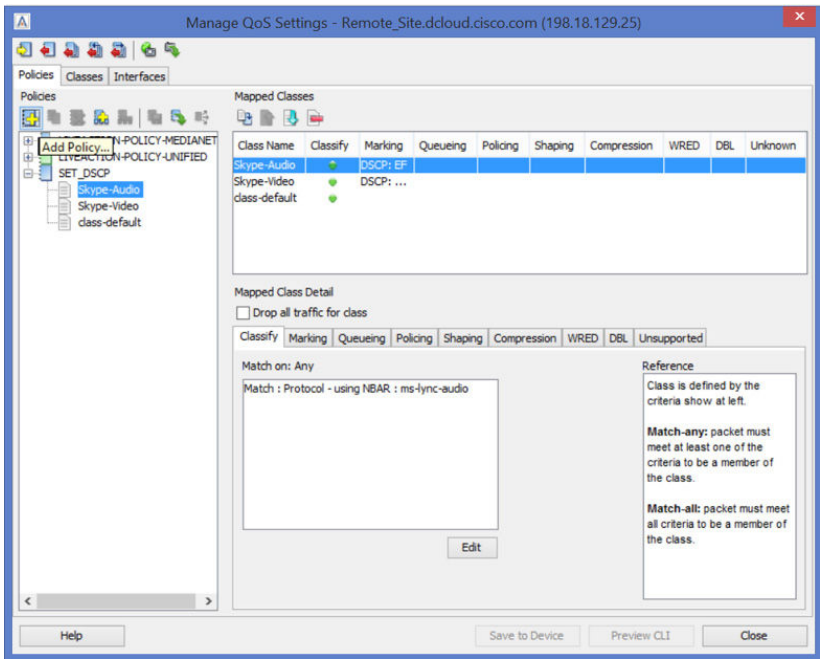
Lastly, select “Save to Device” to apply the policy to the device itself.



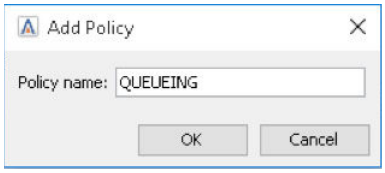
APPENDIX D: SKYPE QOS QUEUING WITH LIVENX AND NBAR2

Now that Skype audio and video were easily identified and marked in the SET_DSCP Policy, create a queuing policy to protect the traffic.

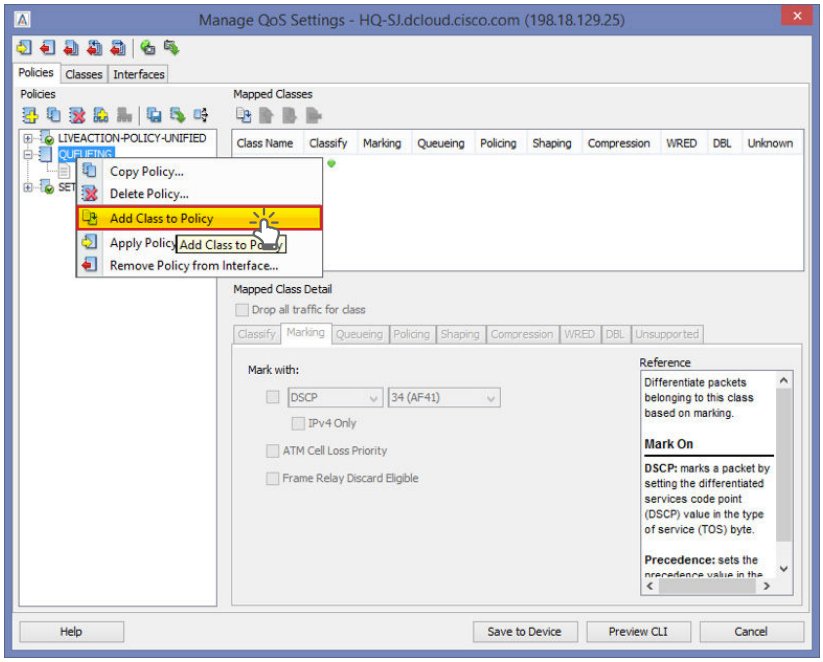
From the “Manage QoS Settings” on the device that would need a queuing policy applied to, start by creating a new policy.



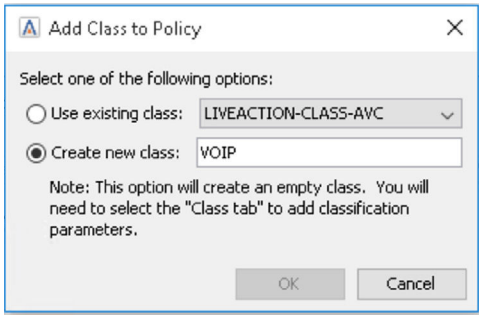
Call the new policy “queuing.”



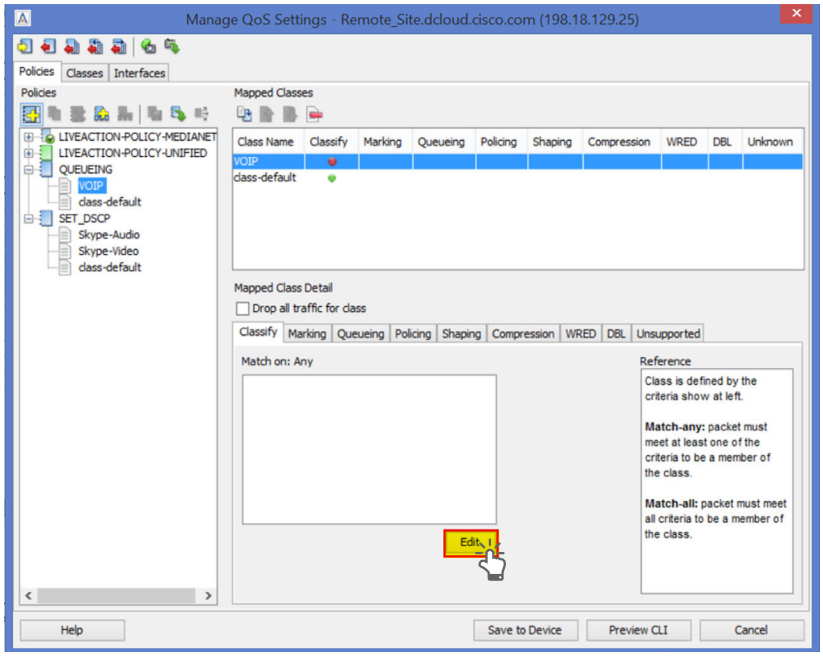
Right click on the new “queuing” policy and select “Add Class to Policy.”



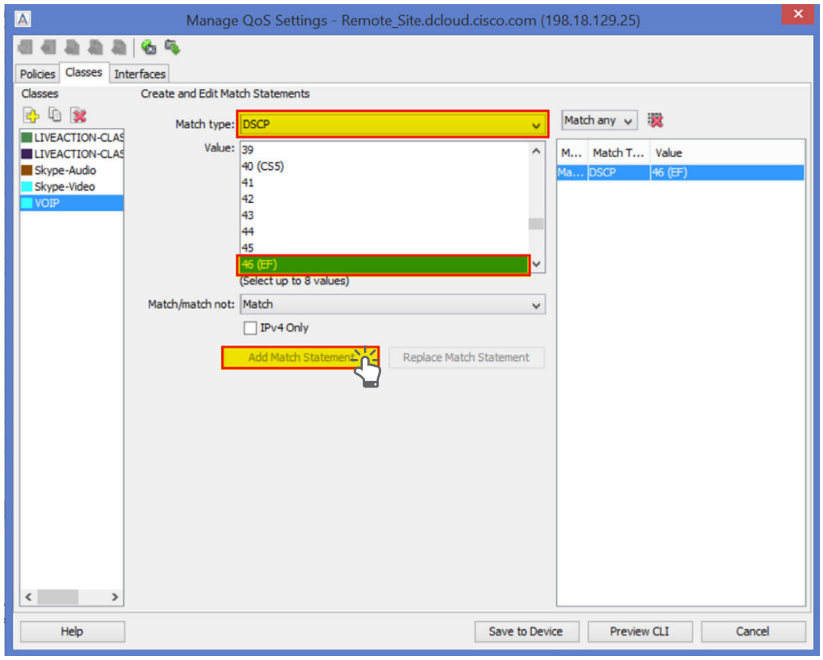
Give the new class a name.



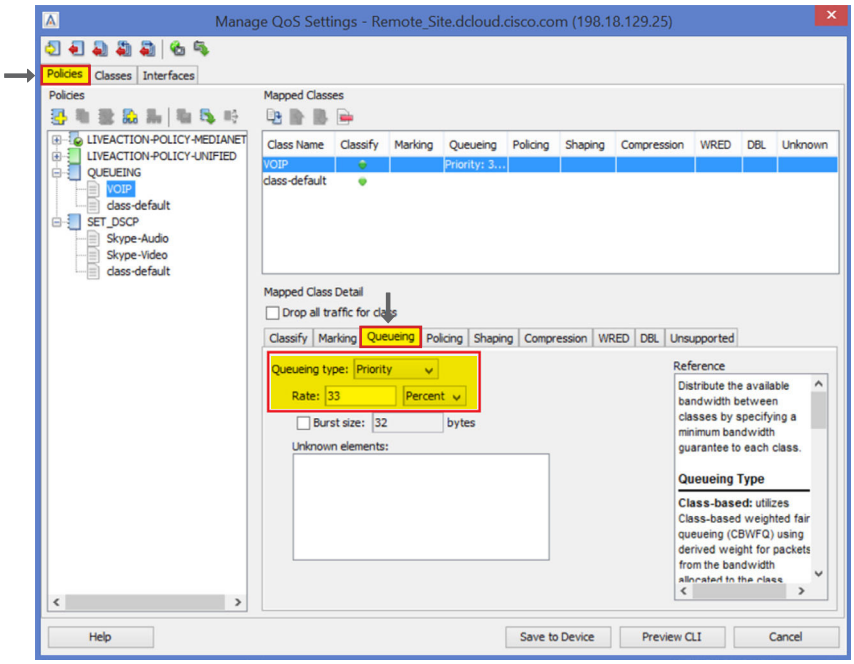
After the new policy is created select “Edit” to match on the DSCP 46 markings.



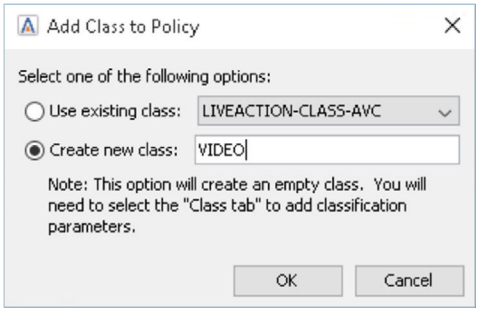
On the “Classes Tab” select “DSCP” as the “Match Type.” Select “46 (EF)” as the value, and then “Add Match Statement” to those markings.



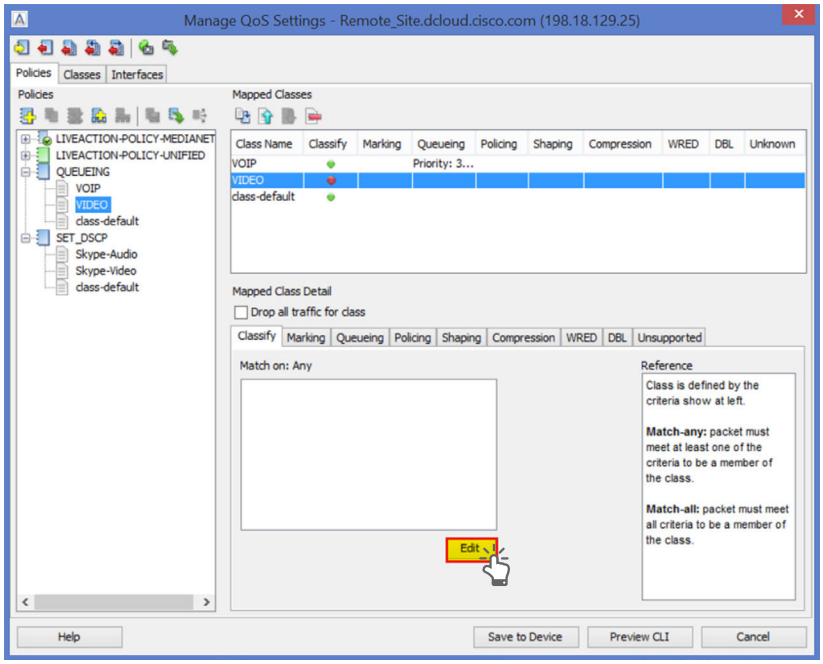
After selecting the correct match type, please go back to the “Policies Tab” and then select the “Queuing Tab” for the VOIP Class. Set the priority bandwidth percentage to 33%. This is a safe starting number for this queue, and can be adjusted by monitoring the queue performance over time.



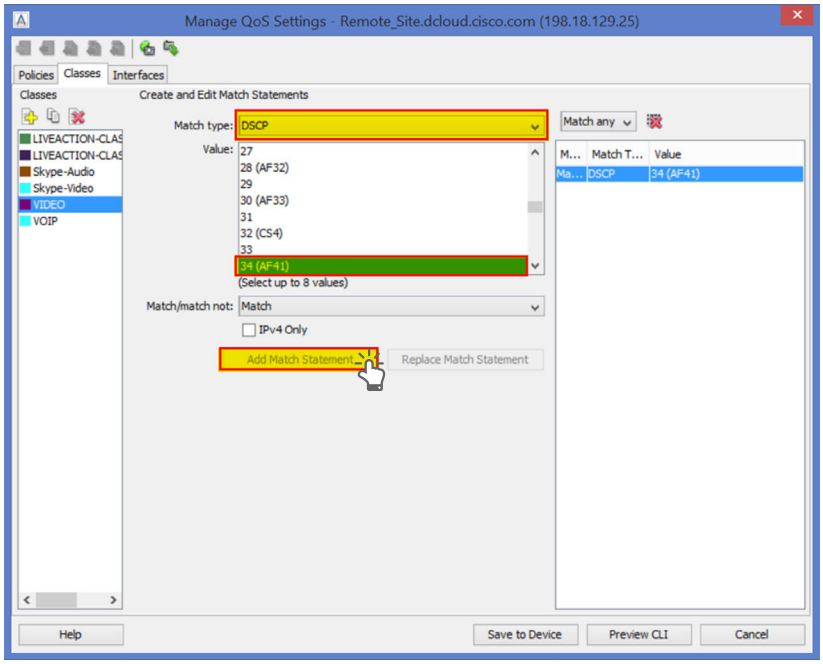
Create a second video class to the policy to protect Skype video.



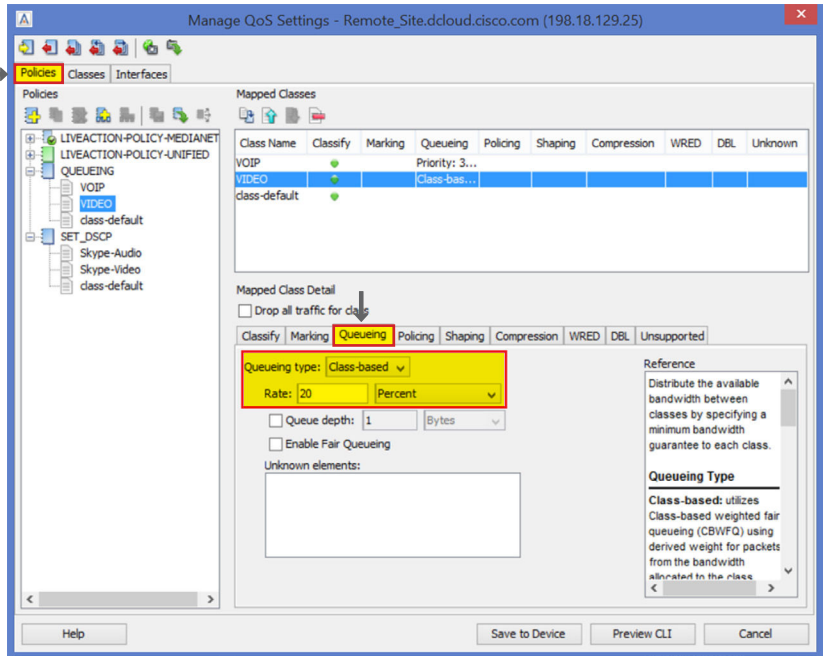
Select “Edit” for to correctly classify video traffic DSCP 34.



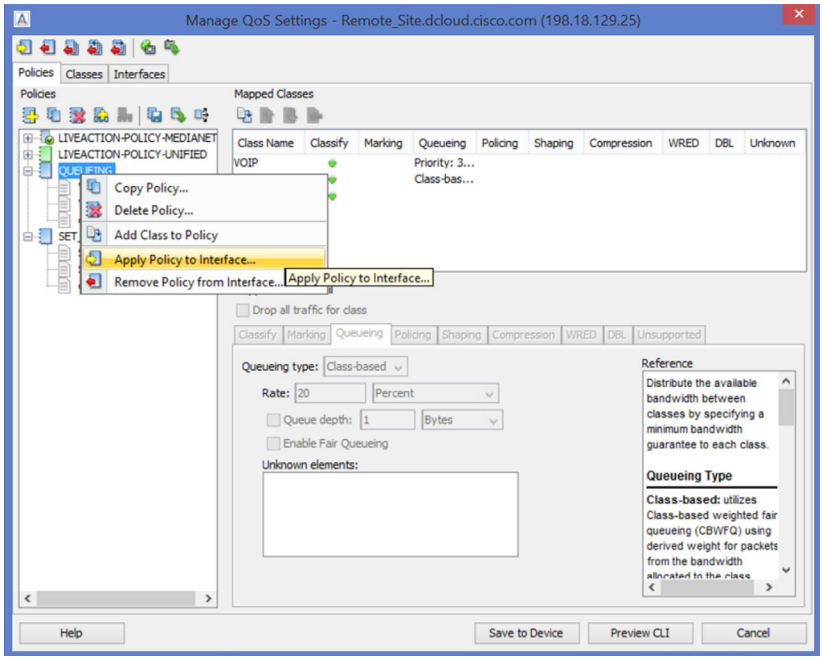
On the classes tab please select “DSCP” as the match type, “34 (AF41)” as the value, then select “Add Match Statement.”



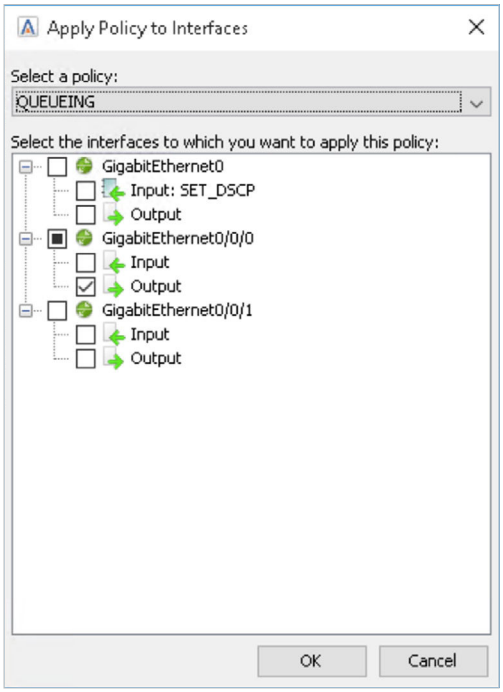
After selecting the correct match type, select the “Policies Tab” and then select the “Queuing Tab” for the video class. Set the bandwidth percentage to 20%. This is a safe starting number for this queue, and can be adjusted by monitoring the queue performance over time.



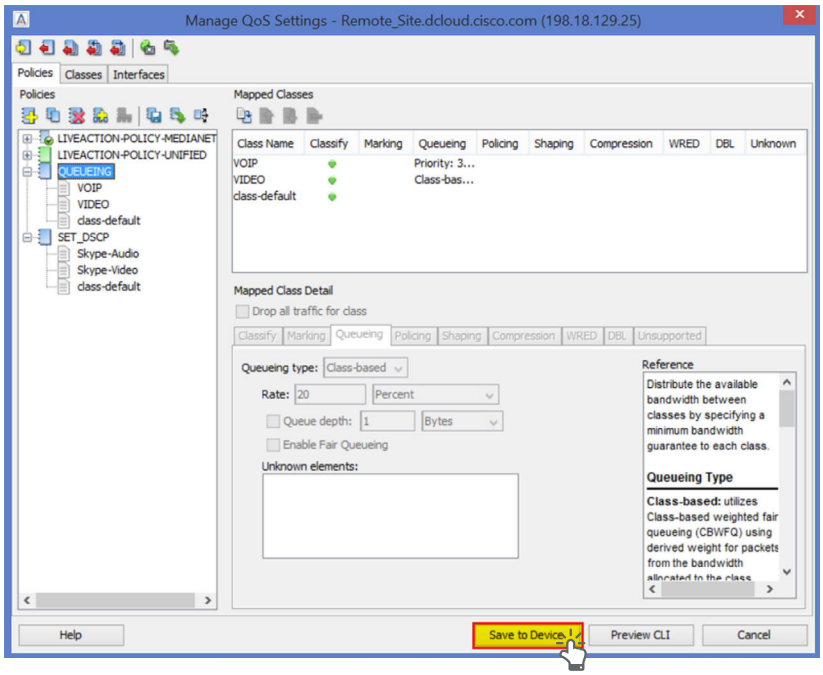
The queuing policy can now be applied to an interface.



Add the policy to the correct interface.



"Save the policy" when completed.



MORE INFORMATION

QoS
Find out more about QoS including best practices and the latest tools for monitoring and creating new policies.

Upcoming Webinars
Check out our updated webinar schedule—gain insights from our special presenters about topics like QoS, Hybrid WAN Management, Capacity Planning and more.

Additional Resources
Case studies, white papers, eBooks and more are available for your learning on the LiveAction resources page.

LiveNX and LiveUX Downloads
Free downloads of LiveNX and LiveUX are available now. Visit our webpage to discover more details and benefits of LiveNX and LiveUX.

ABOUT LIVEACTION

LiveAction provides comprehensive and robust solutions for Network Performance Management. Key capabilities include Cisco Intelligent WAN visualization and service assurance, best-practice QoS policy management, and application-aware network performance management. LiveAction software's rich GUI and visualization provide IT teams with a deep understanding of the network while simplifying and accelerating management and troubleshooting tasks.

LiveAction, Inc. · 3500 West Bayshore Road · Palo Alto, CA 94303 · USA · +1 (888) 881-1116